

KESKITETYSTI HALLITTAVAT WLAN-VERKOT

LAHDEN AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Syksy 2009
Matti Sipilä

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

SIPILÄ, MATTI: Keskitetysti hallittavat WLAN-verkot

Tietoliikennetekniikan opinnäytetyö, 51 sivua

Syksy 2009

TIIVISTELMÄ

Opinnäytetyön tavoitteena on keskitetysti hallittavan WLAN-järjestelmän toteuttaminen Lahden kaupungin Mastonet-verkkoon. Keskitetysti hallittavalla WLAN-järjestelmällä pystytään päivittämään verkon laitekanta vastaamaan tämän päivän haasteisiin. Toteutettava järjestelmä valitaan tutustumalla eri valmistajien järjestelmiin ja testaamalla niiden ominaisuuksia. Lisäksi työssä verrataan perinteisten WLAN-verkkojen toimintaa MESH-verkkoon ja tutkitaan MESH-verkon sopivuutta Mastonet-verkon käyttöön.

Opinnäytetyön teoriaosuudessa käydään läpi WLAN-standardien kehitystä, tulevia WLAN-standardeja, keskitetyn hallinnan protokollia ja valmistajien keskitetyn hallinnan järjestelmiä. WLAN-verkot ovat kulkeneet pitkän matkan 1980-luvun standardoimattomista verkoista 2000-luvun standardoituihin ja keskitetysti hallittaviin WLAN-verkkoihin. Alkuvuodesta 2011 julkaistava Wireless MESH-standardi mahdollistaa vikasietoisen langattoman runkoverkon rakentamisen WLAN-verkon tukiasemien välille.

Keskitetysti hallittavista WLAN-kontrollerijärjestelmistä valittiin tutkittaviksi järjestelmiksi Cisco Systemsin, D-Linkin, Meru Networksin ja Motorolan laitteistot. Lisäksi Ciscon ja D-Linkin WLAN-kontrollerijärjestelmät asennettiin käytössä olevaan testiympäristöön kattavampia testejä varten. Laitteistojen ominaisuudet eivät juuri eronneet toisistaan, ja suuremmat erot järjestelmien välille tulivat hinnan perusteella ja hallintapalvelimen suhteella, jota D-Link ja Meru eivät sisältäneet.

Opinnäytetyön käytännön osuus koostui eri valmistajien laitteiden testauksesta ja niiden vertailusta sekä valitun järjestelmän käyttöönotosta. MESH-järjestelmä osoittautui liian kalliiksi toteutustavaksi tämänhetkiseen Mastonet-verkkoon.

Työn tavoitteena oli saada toimiva keskitetysti hallittava WLAN-järjestelmä käyttöön Mastonet-verkkoon. Tässä tavoitteessa onnistuttiin. Keskitetysti hallittavaksi WLAN-järjestelmäksi valikoitui Cisco Systems 4400 -sarjan kontrolleriin perustuva järjestelmä, josta tehtiin valmis kokoonpano käyttöön otettavaksi, kunhan järjestelmän vaatimat verkkoyhteydet saadaan toimintaan.

Avainsanat: WLAN, kontrolleri, tukiasema, MESH

Lahti University of Applied Sciences
Degree Programme in Information Technology

SIPILÄ, MATTI: Centrally controlled WLAN networks

Bachelor's Thesis in telecommunications, 51 pages

Fall 2009

ABSTRACT

The objective of this thesis was to select a centrally controlled WLAN network system for Mastonet, the wireless network of the city of Lahti, and take it to use. Another objective was to study a wireless mesh network called MESH and to determine whether it is suitable for Mastonet.

The theory part of the thesis presents wireless network standards, the upcoming MESH standard, centrally controlled protocols and different vendors of centrally controlled WLAN systems. It describes what differences there are between the standards and what improvements come with a centrally controlled system. Also it introduces the upcoming wireless MESH standard, which allows wireless backbones to WLAN networks.

The vendors of centrally managed WLAN systems compared were Cisco Systems, D-Links, Meru Networks and Motorola's systems. Cisco Systems and D-Link WLAN controllers were selected to the practical tests. No huge differences were found between the systems except the price and the management server, which is not yet included in the D-Link and Meru systems.

In the practical part, the systems were tested, the test results were compared and the selected system was taken to use. The MESH network turned out too expensive and its backbone connection was too slow for implementation in Mastonet now.

The goal was to get a centrally controlled WLAN system to use in Mastonet and that goal was achieved. The system will be based on Cisco Systems 4400-series WLAN controller. WLAN controller was configured ready to take in use when all network connections have been established.

Key words: WLAN, Controller, Access Point, MESH

SISÄLLYS

1	JOHDANTO	1
1.1	Työn tausta	1
1.2	Työn tavoitteet	1
2	WLAN-STANDARDIT	3
2.1	Langattomat lähiverkot	3
2.2	802.11-standardit	4
2.3	802.11-standardien tulevaisuus	7
2.4	802.11s MESH	8
3	WLAN-VERKON KESKITETTY HALLINTA	10
3.1	Keskitetyn hallinnan edut	10
3.2	CAPWAP-protokolla	11
3.3	LWAPP-protokolla	14
4	ERI VALMISTAJIEN WLAN-JÄRJESTELMÄT	15
4.1	Cisco	15
4.2	D-Link	16
4.3	Muut laitevalmistajat	17
5	TOTEUTETUT TESTIYMPÄRISTÖT	20
5.1	Testiympäristön kuvaus	20
5.2	Cisco-ympäristö	22
5.3	D-Link-ympäristö	23
5.4	MESH-ympäristö	26
5.5	MESH ja WLAN -ympäristöjen vertailu	27
5.6	Testitulokset	28
6	CISCO-JÄRJESTELMÄN KÄYTTÖÖNOTTO	30
6.1	Toteutusympäristön kuvaus	30
6.2	WCS-palvelimen asennus	31
6.3	Kontrollerin käyttöönotto	34
6.4	Tukiasemien liittäminen kotrolleriin	44
6.5	WCS-palvelimen kartta- ja raporttiominaisuudet	47
7	YHTEENVETO	50
	LÄHTEET	52

SANASTO

CAPWAP	Control and Provisioning of Wireless Access Points. Protokolla, jota käytetään tukiasemien ja WLAN-kontrollereiden välisissä yhteyksissä.
CCK	Complementary Code Keying. Langattomassa lähiverkossa käytetty modulaatiotapa.
DHCP	Dynamic Host Configuration Protocol. Verkkoprotokolla, jonka tehtävänä on jakaa IP-osoitteita lähiverkkoon kytkeytyville laitteille.
DoS	Denial of Service. Palvelunestohyökkäys, jonka tavoitteena on verkkopalvelun toiminnan estäminen.
ETSI	European Telecommunications Standards Institute. Eurooppalainen telealan standardisointijärjestö.
HIPERLAN	High Performance Radio Local Area Network. ETSI:n määrittelemä langaton lähiverkko -standardi.
HTTP	Hypertext Transfer Protocol. Www-sivujen siirtämiseen käytettävä tiedonsiirtoprotokolla.
HTTPS	Hypertext Transfer Protocol Secure. HTTP-protokollan salattu versio.
IEEE	Institute of Electrical and Electronics Engineers. Kansainvälinen sähköinsinööriliitto.
ISM	Industrial, Scientific and Medical. Radiotaajuuskaista, jonka käyttö on vapaata teollisuuden, tieteen ja lääketieteen sovelluksiin.
IETF	Internet Engineering Task Force. Internet-verkkoon liittyvien protokollien standardointijärjestö.

LACP	Link Aggregation Control Protocol. Protokolla, jonka avulla verkko-laitteet voivat neuvotella useiden fyysisten porttien liittämistä yhdeksi loogiseksi portiksi.
LAG	Link Aggregation Group. Ciscon nimitys useiden fyysisten porttien liittämistä yhdeksi loogiseksi portiksi. Ei ole LACP-protokollan mukainen.
LAN	Local Area Network. Rajoitetulla maantieteellisellä alueella kuten rakennuksessa toimiva lähiverkko.
LWAPP	Lightweight Access Point Protocol. Protokolla, jota käytetään tietoliikenteeseen tukiasemien ja WLAN-kontrollereiden välillä.
MAC	Medium Access Control layer. OSI-mallin tiedonsiirtokerroksen osakerros. Sisältää laitteen MAC-osoitteen.
MAN	Metropolitan Area Network. Kaupunkiverkko, joka sisältää yhden tai useampia LAN-verkkoja ja toimii esimerkiksi kaupungin alueella.
Mb/s	Megabittiä sekunnissa. Tiedonsiirtonopeus megabiteinä sekunnissa.
MAP	MESH Access Point. MESH-verkon tukiasema, jolla ei ole kaapeloitua runkoyhteyttä.
MIMO	Multiple Input Multiple Output. Antennitekniikka, jossa lähettämiseen ja vastaanottamiseen käytetään useaa antennia.
OFDM	Orthogonal Frequency Division Multiplexing. Monikantaaltomodulointitekniikka, joka perustuu tiedon jakamiseen usealle alikantaallolle.
PBCC	Packet Binary Convolutional Coding. Langattomassa lähiverkossa käytetty modulaatiotapa.

PSK	PreShared Key. Etukäteen käyttäjille jaettu WLAN-verkon salausavain.
QoS	Quality of Service. Tietoliikennepalvelun laadun luokittelu ja priorisointi kiireellisyyden perusteella.
RAP	Root Access Point. MESH-verkon runkotukiasema, jolla on kaape-loitu runkoyhteys ja joka jakaa runkoyhteyttä langattomasti MAP-tukiasemille.
RF	Radio Frequency. Radiotaajuus.
RFMS	RF Management System. Motorolan WLAN-verkkojen hallintapalvelin.
SSID	Service Set Identifier. Langattoman verkon tunnus/nimi.
U-NII	Unlicensed National Informational Infrastructure. 5 GHz:n alueella oleva lisensoimaton taajuuskaista.
VLAN	Virtual Local Area Network. Virtuaalinen lähiverkko.
WCS	Wireless Control System. Ciscon WLAN-verkkojen hallintapalvelin.
WEP	Wired Equivalent Privacy. Langattomien lähiverkkojen tietoturvaprotokolla.
WiFi	Wireless Fidelity. Termi, jota käytetään markkinointinimenä langattomille lähiverkoille.
WiSM	Wireless Service Module. Ciscon nimitys kytkimeen ja reitittimeen integroitavalle kontrollerimoduulille.
WLAN	Wireless Local Area Network. Langaton lähiverkko, jossa verkkolaitteet voidaan yhdistää toisiinsa langattomasti. Yleisesti käytetään tarkoittamaan IEEE 802.11 -standardia.

- WPA Wi-Fi Protected Access. Langattomien lähiverkkojen tietoturvaprotokolla.
- WPA2 Wi-Fi Protected Access 2. Standardin IEEE 802.11i mukainen langattomien lähiverkkojen tietoturvaprotokolla.

1 JOHDANTO

1.1 Työn tausta

Lahdessa vuodesta 2005 toiminut Mastonet on Lahden kaupungin toteuttama ilmainen langaton kaupunkiverkko. Mastonet-verkko on toteutettu yhdistämällä Lahden kaupungin kouluille toteuttama langaton verkko Lahti Energia Oy:n rakentamaan alun perin kaupallisen langattomaan verkkoon. Ajatuksena on ollut tarjota kaupunkilaisille ja Lahdessa vieraileville henkilöille ilmainen langaton Internet-yhteys. Verkon tukiasemat sijaitsevat koulujen katoilla, korkeimpien rakennusten katoilla ja Lahti Energian voimalaitosten piipuissa. Lahti Energia vastasi verkon ylläpidosta vuoden 2008 loppuun asti, jolloin ylläpito siirtyi Lahden ammattikorkeakoululle. Jatkossa verkon kuuluvuutta pyritään parantamaan ns. HotSpot-alueilla, joissa liikkuu paljon ihmisiä, kuten satamassa, kauppatorilla, urheilukeskuksessa, linja-auto- ja rautatieasemalla.

1.2 Työn tavoitteet

Mastonet-verkko sisältää noin 90 WLAN-tukiasemaa. Tukiasemien suuri määrä muodostaa haasteen verkon tukiasemien ylläpidolle. Koska Mastonet-verkossa ei ole käytössä tukiasemien keskitettyä hallintaa, tulee kaikki muutokset toteuttaa jokaiseen tukiasemaan erikseen. Kasvanut tukiasema määrä on lisännyt ylläpidon työtaakkaa, koska yksi muutos verkon parametreihin on tarkoittanut parametrin muuttamista käsin verkon jokaiseen tukiasemaan ja lisäksi tukiasemien tilan seuranta on tukiasemien suuren määrän vuoksi vaikeampaa. Langattomien verkkojen hallinnan ongelmiksi onkin muodostunut viime vuosien aikana muutosten tekemisen vaikeus, yhtenäisten konfiguraatioiden hallinnan puuttuminen, kattavien tilastointitietojen saatavuus, uusien tukiasemien asennustyön määrä ja asetusten vaikea muuttaminen.

Verkon hallintaa helpottamaan laitevalmistajat ovat viime vuosina pyrkineet tuomaan markkinoille erityisiä WLAN-kontrollereita tai WLAN-kytkimiä, joihin on keskitetty verkon kaikki äly. Kontrollerilla pystytään sijoittamaan verkon hallinta keskitetysti yhteen laitteeseen. Näin pystytään helpommin hallitsemaan verkkoja ja seuraamaan langattomien verkkojen kuormitusta. WLAN-kontrollerijärjestelmät ovat helpottaneet tukiasemien lisäämistä verkkoon, asetusten muuttamista, tilastointitietojen keräämistä ja konfiguraatioiden hallintaa.

Tämän opinnäytetyön päätavoitteena on vertailla ja testata eri valmistajien keskitetysti hallittavia kontrolleripohjaisia WLAN-järjestelmiä. Vertailujen ja testien tavoitteena on oppia ymmärtämään WLAN-kontrollerijärjestelmiä ja valita näistä sopivin järjestelmä Mastonet-verkkoon käyttöönotettavaksi.

Toisena tavoitteena on tutustua tulevaan MESH-standardiin sekä testata käytännössä standardia hyödyntävää laitteistoa ja verrata sitä perinteiseen WLAN-järjestelmään. MESH-verkon testien perusteella on tarkoitus tutkia tekniikan soveltuvuutta Mastonet-verkon käyttöön.

Opinnäytetyön käytännön tavoitteena on myös testien perusteella valitun järjestelmän käyttöönotto Mastonet-verkon tuotantoympäristössä ja toteutetun asennuksen dokumentoiminen ja testaaminen.

2 WLAN-STANDARDIT

2.1 Langattomat lähiverkot

Langattomilla lähiverkoilla eli WLANeilla (Wireless Local Area Network) voidaan kytkeä langattomasti tietokoneet ja mobiilit päätelaitteet tietoverkkoon. Langattomien lähiverkkojen käyttö on lisääntynyt räjähdysmäisesti 2000-luvun kuluessa langattomien verkkojen tiedonsiirtonopeuksien kasvaessa ja niiden laitteiden määrän lisääntyessä, jotka voivat hyödyntää langatonta lähiverkkoa. Kohta lähes jokaisella suomalaisella on kännykkä, jolla pystyy kytkeytymään langattomaan lähiverkkoon, ja useammassa kuin joka toisessa taloudessa on kannettava tietokone, jolla voidaan kytkeytyä langattomasti tietoverkkoon.

1980-luvun puolivälissä markkinoille tekivät tuloaan ensimmäiset langattomat lähiverkkotekniikat. Näiden ensimmäisten langattomien lähiverkko tekniikoiden suurimpia ongelmia olivat yhteisen standardin puuttuminen ja laitteiden kallis hinta. Yhteisen standardin puuttuminen aiheutti sen, että tekniikat olivat valmistajakohtaisia eivätkä eri valmistajien laitteet toimineet keskenään. Laitteiden korkea hintataso tarkoitti taas sitä, että langaton lähiverkko ei ollut tavallisen käyttäjän saavutettavissa. (Puska 2005, 15.)

Langattomille lähiverkoille on olemassa kaksi päästandardia: IEEE:n (Institute of Electrical and Electronics Engineers) standardoima 802.11 ja ETSI:n (European Telecommunications Standards Institute) standardoima HiperLAN (High Performance Radio Local Area Networks). Käytännössä IEEE:n 802.11-standardilla on monopoli langattomissa lähiverkoissa, ja puhuttaessa WLAN-verkoista tarkoitetaan 802.11-standardin mukaisia verkkoja. (Wikipedia 2009g.)

2.2 802.11-standardit

IEEE 802.11 on IEEE:n standardi langattomille lähiverkoille. Koska tekniikka on läheistä sukua Ethernetin 802.3-standardille, niin varsinkin alkuaikoina käytettiin usein nimitystä langaton Ethernet. Nykyään käytetään joko markkinointinimeä WiFi (Wireless Fidelity, joka ei varsinaisesti tarkoita yhtään mitään) tai nimitystä WLAN. (Wikipedia 2009a; Wikipedia 2009b.)

Vuonna 1990 IEEE:n LAN/MAN-standardointiryhmä aloitti standardin kehittämisen langattomalle lähiverkolle. Vuoden 1997 heinäkuun lopulla IEEE julkaisi ensimmäisen standardinsa langattomille lähiverkoille, joka oli nimetty 802.11-standardiksi. (Puska 2005, 15.)

802.11 määrittelee pääasiassa OSI-mallin fyysisen kerroksen ja siirtokerroksen alemman osan eli MAC-kerroksen (Media Access Control). Standardi määrittelee verkkoyhteyden nopeuksiksi 1 ja 2 megabittia sekunnissa. 802.11 toimii 2,4 GHz:n vapaalla ISM-taajuusalueella (Industrial Scientific Medical), ja se määrittelee välitystekniikoiksi infrapunaa ja radiotien. ISM-taajuusalueet ovat maailmanlaajuisesti lupavapaita radiotaajuuskaistoja, jotka on alun perin tarkoitettu teolliseen, tieteelliseen ja lääketieteelliseen käyttöön. Eräs yleisin tällainen 2,4 GHz:n ISM-kaistalla toimiva laite on lähes joka kotitaloudesta löytyvä mikroaaltouuni. ISM-taajuuskaistat Suomessa ovat

- 6765 - 6795 kHz
- 13553 - 13567 kHz
- 26957 - 27283 kHz
- 26957 - 27283 kHz
- 40,660 - 40,700 MHz
- 902 - 928 MHz
- 2400 - 2500 MHz
- 5725 - 5875 MHz
- 24,000 - 24,250 GHz
- 61,0 - 61,5 GHz
- 122 - 123 GHz
- 244 - 246 GHz.

(Puska 2005; Wikipedia 2009d; Viestintävirasto 2009.)

Pari vuotta alkuperäisen 802.11-standardimäärittelyn jälkeen IEEE julkaisi syksyllä 1999 kaksi uutta standardimäärittelyä (802.11b ja 802.11a). Jatkuvasti kehittyneet verkkosovellukset ja langattomien verkkojen yleistymisen ja lisääntyneen käyttö aiheuttivat sen, että 802.11-standardin määrittämät tiedonsiirtonopeudet jäivät liian hitaiksi ja tarvittiin uusi standardi, joka vastaisi paremmin käyttäjien ja sovellusten asettamiin haasteisiin. (Puska 2005, 15.)

Vastauksena asetettuihin haasteisiin IEEE ratifioi uuden 802.11b-standardin. Standardi määrittelee uusiksi verkkoyhteyden nopeuksiksi 5,5 Mb/s ja 11 Mb/s, mikä tekee 802.11b:stä huomattavasti edeltäjäänsä nopeamman. Yhteys toimii edelleen samalla 2,4 GHz:n ISM-taajuudella, mutta käyttää siirtotekniikkana CCK-tekniikkaa (Complement Code Keying). Tämä tarkoittaa, että tieto lähetetään 64:nä 8-bittisen koodisanan sarjoina. Sarjamuodossa kullakin koodisanalla on oma matemaattinen merkityksensä. Vaihtoehtoisena siirtotekniikkana 802.11b tarjoaa PBCC-tekniikan (Packet Binary Convolutional Coding). PBCC tarjoaa 64-tilaisen koodauksen, joka tarjoaa suorituskyvyn kannalta paremman signaalikohinasuhteen, mutta vaatii enemmän signaalin prosessointikykyä. (Puska 2005, 15; Heegard & Shoemake 2004.)

Jälkimmäinen uusista standardeista oli 802.11a, joka käyttää 5GHz U-NII-taajuuksia (Unlicensed National Informational Infrastructure). Koska U-NII-taajuudet oli varattu standardin julkistamisen aikaan muihin käyttötarkoituksiin Euroopassa, on standardin merkittävimäksi käyttöalueeksi jäänyt USA ja Kanada, vaikka nykyään 802.11a:ta voidaan käyttää tietyin rajoituksin Euroopassa. 802.11a-standardin lisäykseksi Euroopan alueelle on jäänyt lähinnä vain se, että standardi esitteli uuden siirtotekniikan OFDM-tekniikan (Orthogonal Frequency Division Multiplexing), joka perustuu signaalien jakamiseen pienempiin alasiinaaleihin. Jaetut signaalit siirretään yhtäjaksoisesti eri taajuuksilla. Nämä muutokset mahdollistivat verkkoyhteyden nopeuden kasvattamisen 54 Mb/s:iin. (Puska 2005, 16.)

802.11a-standardi ei ole eduistaan huolimatta kokenut 802.11b:n kaltaista suosiota. Tähän on ollut syynä hinnoiltaan kalliimmat verkkolaitteet ja korkeamman taajuuden aiheuttama kantaman pientyminen verrattuna samoissa oloissa käytettyyn 802.11b-standardin tekniikkaan. (Puska 2005.)

Vuonna 2003 IEEE ratifioi tutkimustyön tuloksena uuden 802.11g-standardinsa. 802.11g-standardi on risteytys 802.11a- ja 802.11b-standardeista. Tekniikaltaan standardi on lähes identtinen 802.11a-standardin kanssa tosin sillä erotuksella, että se toimii 802.11b-standardin kanssa 2,4 GHz:n alueella ja tarjoaa tiedonsiirtoon vaihtoehdoksi OFDM-tekniikalle CCK-tekniikan. OFDM-tekniikalla 802.11g pystyy liikennöimään 6, 9, 12, 18, 24, 36, 48 ja 54 Mb/s nopeuksilla sekä vanhempien 802.11- ja 802.11b-standardien käyttämällä tiedonsiirto tekniikoilla 1, 2, 5,5 ja 11 Mb/s nopeuksilla. 802.11g käyttää 2,4 GHz:n taajuutta ja tukee myös vanhempia modulointitekniikoita, ja on siksi täysin yhteensopiva vanhemman 802.11b-standardin kanssa. Jos 802.11g verkossa on yksikin 802.11b:tä hyödyntävä laite, hidastuu verkko osittain 802.11b:n tasolle eikä parasta verkon suorituskykyä saavuteta. (Granlund 2007, 305; Wikipedia 2009c.)

802.11g-standardi on käytännössä syrjäyttänyt vanhemman b-standardin yleisessä käytössä. 802.11g-laitteet sopivat paikkoihin, joissa vaaditaan suurta kaistaa, esimerkiksi messuhalleihin tai auditorioihin. (Granlund 2007, 305.)

Vuoden 2004 alussa IEEE perusti työryhmän, jonka tehtävänä oli luoda uusi langaton standardi 802.11n (High-Throughput) joka standardoitiin syyskuussa 2009. Tavoitteeksi asetettiin noin 200 Mb/s keskimääräinen nopeus ja 540 Mb/s huippunopeus sekä 50 % suurempi kantama. Yhteys perustuu MIMO-antennitekniikkaan (Multiple Input Multiple Output), jossa käytetään useampaa antennia ja useampaa kanavaa yhtä aikaa. Siirtotekniikkana käytetään OFDM-tekniikkaa. (Granlund 2007, 305.)

802.11-standardiin on esitelty useita laajennuksia täydentämään päästandardeja. 802.11e-laajennus sisältää toimintoja verkon palvelunlaadun QoS (Quality of Service) kehittämiseksi. 802.11d-laajennus sisältää uusia kenttiä tukiasemien levitysviesteihin, joilla kerrotaan laitteen sijaintimaa. Ajatuksena on se, että langaton laite osaa itse valita tämän tiedon mukaan taajuuskaistan, jota kyseisen tukias-

man alueella on luvallista käyttää. Merkittävä etu tästä on paljon matkustaville ihmisille, joiden langattomat laitteet pystyvät automaattisesti valitsemaan kunkin maan standardin, esimerkiksi 802.11a Pohjois-Amerikassa ja 802.11g Euroopassa. (Wikipedia 2009a; Wikipedia 2009b.)

802.11h -laajennus sisältää muutoksia 5 GHz:n taajuusalueella toimiville langattomille laitteille Euroopassa, jossa aikaisemmin kyseinen taajuus oli varattu muun muassa satelliittiliikenteelle. 802.11i-laajennus parantaa aikaisemmin osittain valmistajakohtaisia tietoturvaominaisuuksia ja määrittelee ne standardin osaksi. 802.11j-standardi määrittelee puolestaan Japanissa käytettävän siirtotekniikan. (Wikipedia 2009a; Wikipedia 2009b.)

2.3 802.11-standardien tulevaisuus

802.11-standardiperheeseen on kehitteillä useita uusia standardeja ja niiden laajennuksia, kuten esimerkiksi 802.11 VHT -työryhmien valmistelemat 802.11ad Extremely High Throughput 60 GHz, joka määrittelee 60 GHz:n taajuudella toimivan siirtotekniikan ja 6 GHz -taajuuden tuntumaan sijoittuvan 802.11ac Very High Throughput <6 GHz. 2,4 GHz:n alueen ahtauteen on pakottanut etsimään uusia taajuusalueita langattomien lähiverkkojen käyttöön; yksi tällainen taajuusalue löytyy 60 GHz:n alueelta. 60 GHz:n alue on ollut tähän asti vähäisellä käytöllä, koska ilman happi vaimentaa signaalia kohtalaisen paljon. 60 GHz:n alueella päästään jo lähelle valokuitunopeuksia; langattomalla verkkotekniikalla tämän mahdollistaa 9 GHz:n levyinen taajuuskaista verraten 2,4 GHz:n noin 100 MHz taajuuskaistaan. Edellä mainittujen standardien kehitys on aloitettu loppuvuodesta 2008, joten ne ovat vasta alkutekijöissään ja arvioitujulkaisu ajankohta on vasta loppuvuodesta 2012. (Leidenius 2008; IEEE 2009.)

Eräs mielenkiintoisimmista tulevista standardeista on 802.11s -laajennus joka sisältää tuen ns. Wireless MESH -verkkojen rakennukseen tukiasemien välillä. Standardi ei ole vielä valmis, mutta IEEE arvioi julkaisevansa sen tammikuussa 2011. (IEEE 2009.)

2.4 802.11s MESH

Vuonna 2004 IEEE alkoi valmistella 802.11s-standardia eli Wireless Mesh -laajennusta. Virallista kutsumanimeä ei ole, vaan on käytetty WMesh- ja MESH-nimityksiä kirjoitusasun vaihdellessa. MESH-standardin tarve on lähtenyt tarpeesta ulottaa langaton lähiverkko alueille, joille tietoliikenneverkko ei ulotu eikä ole mahdollista toteuttaa kustannusteknisesti järkevästi. Joitakin esimerkkejä kohteista, joissa MESH:iä voidaan hyödyntää:

- suuret ulkokentät, joilla liikkuu ja viettää aika paljon ihmisiä
- tilapäinen kapasiteetin lisääminen ulkoilmatapahtumissa, jotka järjestetään samoissa paikoissa säännöllisesti, kuten urheilukilpailut
- erilaiset messut ja ulkoilmatapahtumat, jotka järjestetään eripaikoissa tai vaikka vaan joka toinen vuosi, kuten Jukolan Viesti, Farmari, Okra, Finn-Metko
- satamat, kuten tuontiauto- ja konttikentät, joille halutaan rakentaa langaton lähiverkko mahdollistamaan kontin tai ajoneuvon sijainnin sähköistä arkistointi. (Hämäläinen 2005; Wikipedia 2009e; Wikipedia 2009f.)

MESH on reitittävä verkko, jossa paketit voivat kulkea useaa eri reittiä kahden pisteen välillä. Yhden reitin katkeaminen ei estä MESH-verkon laitteiden välistä kommunikaatiota. Kun reitti havaitaan katkenneeksi, käytetään toissijaista reittiä laitteiden välillä. Standardin mukainen MESH-verkko koostuu kolmen laisista osista: verkossa on aina yksi kontrolleri, jokaista runkopistettä kohden on RAP-tukiasema (Root Access Point) ja n kappaletta MAP-tukiasemia (MESH Access Point). (Hämäläinen 2005; Wikipedia 2009e; Wikipedia 2009f.)

MESH-verkko on aina kontrolleriperustainen, eli verkon kaikki äly on keskitetty kontrolleriin, jolla hallitaan koko verkkoa. MESH-verkkoa ei ole mahdollista toteuttaa ilman kontrolleria, koska tukiasemassa ei yleensä ole konsoliporttia ja web-konfiguraatiomahdollisuutta. Kontrolleri hoitaa automaattisesti verkon konfiguroinnin, kuten taajuusasettelun ja MESHin määrittelyn, kun RAP-tukiasema kytketään samaan lähiverkkoon kontrollerin kanssa ja MAP-tukiasemassa on virrat kytkettynä RAP-tukiaseman kuluvuusalueella. Ylläpitäjälle ei jää muuta kuin langattomien verkkojen määrittely ja toiminnan toteaminen. Koska verkon kaikki

äly on kontrollerissa, on MESH-verkon tukiasemat pelkkiä radio-osia, tosin RAP-tukiasemassa on verkkokytkeä, kuten Ciscon 1520-sarjan tukiasema voidaan varustaa yhdellä viiva neljällä gigabitin ethernetliitännällä tai valokuituliitännällä. MESH-tukiasema on yleensä varustettu kahdella tai kolmella radiolla, joista yksi on 2,4 GHz alueella toimiva b/g radio, johon clientit kytkeytyvät ja toinen tai muut on 5 GHz:n alueella toimivia MESH-radioita tukiasemien välisiä runkoyhteyksiä varten. (Hämäläinen 2005; Wikipedia 2009e; Wikipedia 2009f.)

MESH muistuttaa rakenteeltaan hyvin paljon GSM-verkkoa. MESH rakentuu soluista, kuten GSM, eikä lähekkäisissä soluissa voida käyttää samaa tai toisiaan häiritseviä vierekkäisiä taajuuksia. MESH:n toiminnassa on hyvin paljon muitakin yhtäläisyyksiä GSM:n kanssa. (Hämäläinen 2005; Wikipedia 2009e; Wikipedia 2009f.)

MESH-verkkoa toteutettaessa on tärkeää huolehtia, että RAP-pisteitä on riittävästi, jotta tiedonsiirto MESH-verkon ja ulkoverkon välillä on joustavaa eivätkä runkopisteet ruuhkautuisi. MESH-verkkoa toteutettaessa suositeltavaa olisi rajoittaa MESH-hyppyjen määrä kolmeen, koska jokainen hyppy runkopisteen ja clientin välillä periaatteessa tuplaa tiedonsiirtoon kuluneen ajan. MESH-tukiasemien kuuluvuusalueiden on oltava päällekkäisiä noin 10–40 %, jotta tiedon puskurointi ja käsittely on mahdollista. Yksittäisen tukiaseman alueella voi olla maksimissaan viisi muuta tukiasemaa. Suuremmalla määrällä pakettien yhteentörmäyksiä tapahtuu liikaa ja MESHin toimivuus heikentyy huomattavasti. (Hämäläinen 2005; Wikipedia 2009e; Wikipedia 2009f.)

3 WLAN-VERKON KESKITETTY HALLINTA

3.1 Keskitetyn hallinnan edut

Suurten yritysten ja yhteisöjen langattomien verkkojen käytön ja käyttäjien määrän kasvu sekä myös niiden alueiden ja tilojen laajentuminen, joissa palvelua halutaan tarjota käyttäjille, asettaa haasteen verkon ylläpidolle. Koska tukiasemalaitteiden määrä kasvaa hyvinkin radikaalisti aluetta kasvatettaessa ja tukiasemat voivat sijaita maantieteellisesti katsottuna hyvin laajalla alueella. Jos tukiasemia hallitaan ilman keskitettyä hallintaa, työmäärä lisääntyy lisääntynyt työmäärä lisää ylläpitohenkilöstön tarvetta, joka nostaa kustannuksia.

Perinteisessä WLAN-ratkaisuissa tukiasema hoitaa liikenteen jakamisen, radiotien kontrolloinnin, tietoturvan sekä muut liikenteenohjaustehtävät, mikä tarkoittaa sitä, että verkon jokainen tukiasema tarvitsee yksilöllisen konfiguraation. Perinteisessä ratkaisussa, jos ylläpitohenkilöstöstä etäällä sijaitseva tukiasema vikaantuu, olisi huoltokeikalle hyvä olla ottaa mukaan varalaitte; jos vikaa ei saakaan korjattua paikan päällä, niin varalaitteella palvelu katkoksesta jäisi mahdollisimman lyhyt. Esimerkiksi kolmen tukiasemalaitteen verkossa jokaiselle laitteelle voisi olla valmiiksi konfiguroitu varalaitte eikä kustannukset vielä karkaisi käsistä. Kymmeniä tukiasemia käsittävässä verkossa vikatilanteen sattuessa varalaitte konfiguroidaan vian ilmetyä muutaman varalaitteen varastosta sopimaan vikaantuneen laitteen paikalle. Todennäköisyys, että useat verkon tukiasemat vikaantuisivat saman aikaisesti, on hyvin pieni, eivätkä läheskään kaikki tukiasemat vikaannu järjestelmän elinaikana ollenkaan.

Tästä seuraa siis se, että mikäli yksittäisiä tukiasemia hallitaan ilman erillisiä etähallintalaitteita, niin se nostaa kustannuksia ja henkilöstömäärää. Myös virhetilanteiden ja verkon kuormituksen havainnointi WLAN-verkossa on vaikeampaa. Verkon käyttäjät eivät voi suorittaa nopeita verkon vaihtoja, mitä vaaditaan esimerkiksi puheen ja kuvan reaaliaikaisessa välityksessä. Fyysisenä riskinä menetelmässä on tukiaseman varastaminen sen paikalta.

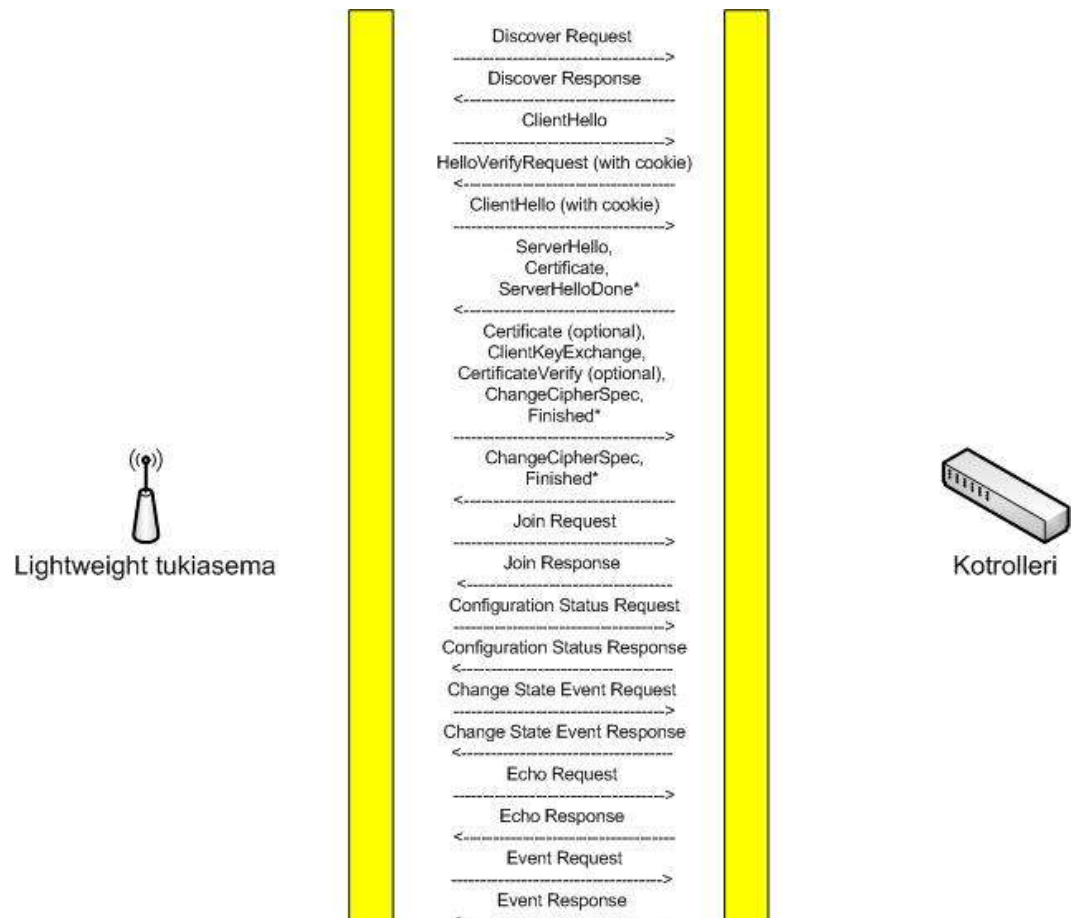
Lightweight-tukiasemien avulla toteutetuissa järjestelmissä WLAN-kontrolleri hoitaa tukiaseman normaalisti suorittamat tehtävät, kuten pääsynhallinnan. Lisäksi voidaan toteuttaa nopea roaming, koska yhteystiedot ovat kontrollerilla, liikenteen hallintaa ja suodattamista sekä QoS-toimintoja (Quality of Service). Kontrolleri mahdollista erittäin suurten verkkojen toteuttamisen ja hallitsemisen, jotka voivat käsittää jopa tuhansia tukiasemia. Lisäksi uusien tukiasemien lisääminen on hyvin helppoa eikä yleensä vaadi konfiguraatioiden tekemistä. Tämän tekniikan edut ovat jo huomattavan käteviä, jos yrityksellä on useita tukiasemia ympäri yrityksen toimitiloja, jotka voivat sijaita eri paikkakunnilla. (Mäkinen 2006.)

3.2 CAPWAP-protokolla

Jos otetaan tukiasemasta kaikki sen äly pois ja sijoitetaan se hallintakeskukseen, kuten kytkin, reititin tai kontrolleri. Teoriassa voidaan rakentaa halvemmalla ja helpommin hallittava VLAN-verkko, joka mahdollistaisi eri valmistajien tukiasemien ja hallintalaitteiden yhdistämisen toisiinsa. Mutta tämä on mahdollista vain, jos laitteet käyttävät samaa standardia keskinäiseen kommunikaatioonsa muussa tapauksessa ollaan sidoksissa tietyn valmistajan laitteisiin. (McKeag 2004.)

Edellä esitettyyn ajatukseen, että eri valmistajien laitteet voisivat toimia yhdessä, teoriassa ainakin ratkaisuna toimii CAPWAP-protokolla (Control and Provisioning of Wireless Access Points), joka on IETF:n standardoima kontrolliprotokolla, jota kontrolleri ja lightweight-tukiasema käyttävät keskinäiseen kommunikointiin. CAPWAP-protokolla on kehitetty käyttämällä runkona LWAPP-protokollaa (Light Weight Access Point Protocol). (Wikipedia 2009h.)

Tukiaseman ja kontrollerin välille muodostetaan CAPWAP-tunneli protokollan määrittämällä kättelyllä, joka on esitetty kuviossa 1. CAPWAP-tunneli muodostuu seuraavasti: Ensimmäisessä vaiheessa CAPWAP-protokollaa tukeva lightweight-tukiasema etsii CAPWAP-etsintämekanismilla kontrollerin lähettämällä *Discover Request* -paketin, jolla tukiasema kysyy, onko verkossa kontrollereita, johon paketin vastaanottanut kontrolleri vastaa *Discover Response* -paketilla. Toisessa vaiheessa, kun tukiasema on löytänyt kontrollerin, aloitetaan kättely, jossa ensin tervehditään *Hello*-paketeilla vaihdetaan sertifikaatit ja avaimet. Kun kättelyvaihe on suoritettu, aloitetaan yhteydenmuodostusvaihe, jossa tukiasema lähettää *Join Request* -paketin, jolla se pyytää lupaa kontrollerilta liittyä siihen ja kontrolleri myöntää luvan liittyä *Join Response* -paketilla. Yhteyden muodostamisvaiheen suorituksen jälkeen suoritetaan konfiguraation vaihtovaihe. Tukiasema pyytää konfiguraatiotiedostot *Configuration Status Request* -paketilla, johon vastauksena kontrolleri lähettää konfiguraatiot *Configuration Status Response* -paketilla. Konfiguraation vaihdon jälkeen varmistetaan konfiguraation vaihdon onnistuminen, jolloin tukiasema lähettää *Change State Event Request* -paketin, johon kontrolleri vastaa *Change State Event Response* -paketilla. Tämän jälkeen CAPWAP-tunneli on muodostunut. Kontrolleri käyttää *Change State Event Response* -pakettia myös tukiaseman radioiden oikeaan tilaan asettamiseen. CAPWAP-tunnelin olemassa ollessa *Echo Request*-, *Echo Response*-, *Event Request*- ja *Event Response* -paketeilla varmistetaan suorituksen aikana tunnelin toimiminen. CAPWAP-tunnelissa kulkee konfiguraatiot, firmwaret, kontrollitiedot ja käyttäjien dataliikenne kontrollerin ja tukiaseman välillä. Käyttäjien kaikki dataliikenne kulkee siis CAPWAP-tunnelissa, ja kontrolleri kytkee käyttäjän oikeaan aliverkkoon ja VLANiin näin käyttäjien liikenne on parhaiten hallittavissa. (Cisco Systems 2009b; Calhoun, Montemurro & Stanley 2009.)



KUVIO 1. Tukiaseman ja kontrollerin välinen CAPWAP-protokollaliikenne (Calhoun ym.)

CAPWAP-protokolla voi toimia OSI-mallin tasoilla 2 ja 3. Tasolla 2 CAPWAP sijaitsee ethernet-kehyksessä, jolloin kontrollerin ja tukiaseman tulee sijaita samassa aliverkossa tai olla suoraan kytkettynä toisiinsa. Tasolla 3 CAPWAP sijaitsee UDP/IP-kehyksessä, jolloin kontrolleri ja tukiasema voivat olla joko suoraan kytkettynä toisiinsa, kytketty samaan aliverkkoon tai sitten kytketty eri aliverkkoihin. CAPWAP-protokollan toiminnan tasolla 3 mahdollistaa se, että tukiasema lähettää DHCP-kyselyn ennen kuin se käynnistää CAPWAP-toiminteet ja DHCP optiolla 43 välitetään DHCP-palvelimelta tukiasemalle kontrollerin IP-osoite, näin tukiasema ja kontrolleri voivat sijaita eri aliverkossa. (Cisco Systems 2009b.)

3.3 LWAPP-protokolla

LWAPP on laitevalmistajien, kuten Airespacen, Ciscon, D-Linkin ja NTT Docomon, yhdessä kehittänyt protokolla, jota lightweight-tukiasema ja kontrolleri käyttävät keskinäiseen kommunikaatioonsa ja liikenteeseensä. Ensimmäinen versio LWAPP:stä julkaistiin jo vuonna 2002. LWAPP:n pohjalta on kehitetty IETF:n standardoima CAPWAP-protokolla, joka on toiminnaltaan samankaltainen kuin LWAPP. LWAPP:n suurin ongelma oli/on sen standardoimattomuus. (Mäkinen 2006, 30–31.)

Uudet kontrollerimallit, jotka on julkaistu CAPWAP:n julkaisun jälkeen, kuten Ciscon 5500 -sarjan kontrolleri, tukevat pelkästään CAPWAP-protokolla, mutta vanhemmissa tuotteissa LWAPP tulee elämään niiden elinkaaren loppuun asti. LWAPP:n ja CAPWAP:n suurin ero on niiden käyttämät UDP-portit. LWAPP-protokollan käyttämät UDP-portit on 12222 ja 12223 ja CAPWAP-protokollan käyttämät UDP-portit on 5246 ja 5247. LWAPP:n ja CAPWAP:n eroista ei löydy juuri muuta tietoa kuin niiden käyttämät UDP-portit. Ymmärrettävää sinänsä valmistajat eivät ole tahtoneet julkaista LWAPP:n tarkkoja speksejä, koska se on heidän oma standardinsa. (Cisco Systems 2009b.)

27.7.2005 julkaistu 3.0.100.5 on vanhin Ciscon kontrolleriohjelmiston versio, jonka Release Notes löytyy osoitteesta:

http://www.cisco.com/en/US/products/ps6366/prod_release_notes_list.html.

3.0.100.5 -ohjelmistoversion Release Notesissa puhutaan jo LWAPP-protokollasta.

24.11.2008 julkaistu Ciscon 5.2.157.0 on ensimmäinen Ciscon kontrolleriohjelmiston versio, jonka mukana tulee tuki CAPWAP-protokollalle. Tuorein versio Ciscon kontrolleriohjelmistosta on 7.11.2009 julkaistu 6.0.188.0

4 ERI VALMISTAJIEN WLAN-JÄRJESTELMÄT

4.1 Cisco

Cisco Systems on hallittavien WLAN-kontrollerijärjestelmien markkinajohtaja. Ciscon kontrollerijärjestelmä koostuu kontrollerista, lightweight-tukiasemista ja valinnaisesta WCS-palvelimesta (Wireless Control System). Ciscolta löytyy kolmeen kategoriaan jaoteltavia lightweight-tukiasemia: on sisätilan, haastavan RF-ympäristön (Radio Frequency) ja MESH-tukiasemia. Ciscon kontrolleri voi olla standalone-laite tai integroituna kytkimen tai reitittimen runkoon.

Ciscon Aironet 1130AG -sarjan lightweight-tukiasemat ovat sisätilan tukiasemia sisäänrakennetulla antennilla ja 802.11a/b/g-radiolla (Cisco Systems 2009c). Ciscon Aironet 1240AG -sarjan lightweight-tukiasemat ovat sisätilan tukiasemia ulkoisilla antenniliittimillä ja 802.11a/b/g-radiolla (Cisco Systems 2009d). Ciscon Aironet 1250 -sarjan lightweight-tukiasema on 1240AG-sarjan tukiaseman uudempi versio, joka tukee 802.11a/b/g-standardien lisäksi 802.11n-standardia (Cisco Systems 2009e). Ciscon 1520-sarjan lightweight-tukiasema mahdollistaa tulevan 802.11s-standardin mukaisen MESH-verkon rakentamisen ja on asennettavissa ulkotiloihin ilman erillistä koteloitua (Cisco Systems 2009f).

Ciscon 2100 -sarjan WLAN-kontrolleri tukee 6-25 tukiasemaa ja sisältää 8 kappaletta 10/100Mb:n verkkoliityntöjä. Ciscon 4400 -sarjan WLAN-kontrolleri on oikeastaan 2100-sarjan järeämpi versio, joka tukee 12:tä, 25:tä, 50:tä tai 100:aa tukiasemaa ja sisältää 2 tai 4 kappaletta gigabitin verkkoliityntöjä. Ciscon 5500 -sarjan WLAN-kontrolleri tukee 250:tä tukiasemaa ja 7 000:tä käyttäjää. Catalyst 6500 -sarjan WiSM (Wireless Service Module) on 6500-sarjan kytkimeen integroitava 4404-kontrollerimoduuli, joka tukee 300:aa tukiasemaa. Catalyst 6509 kytkinrunko tukee seitsemää WiSM-moduulia eli saavutetaan tuki 2100 tukiasemalle. Cisco 7600 -sarjan WiSM-reitittimeen integroitava 4404-kontrollerimoduuli tukee 300:aa tukiasemaa ja 7609 reititinrunko tukee seitsemää WiSM-moduulia. (Cisco Systems 2009b.)

Ciscon kehittämä WCS (Wireless Control System) on täydellinen alusta järjestelmänlaajuiseen WLAN-hallintaan. WCS mahdollistaa WLAN-verkkojen helpon konfiguroinnin, valvonnan ja hallinnan. WCS mahdollistaa tämän kaiken kontrollereille sekä standalone-tukiasemille. Ciscon WCS:llä voidaan hallita järjestelmät aina yhden kontrollerin järjestelmästä järjestelmiin, joissa on 3 000 lightweight-tukiasemaa, 1 250 standalone-tukiasemaa ja 750 WLAN-kontrolleria. WCS-järjestelmä kannattaa ottaa käyttöön viimeistään siinä vaiheessa kun langaton verkko sisältää useita kontrollereita ja suuren määrän tukiasemia. WCS toimii serverialustalle upotetussa tietokannassa. (Cisco Systems 2009a.)

WCS:llä voidaan valvoa verkkoa täysin reaaliaikaisesti sen tarjoamalla lukuisilla eri raporteilla verkon käyttöasteesta, asiakastiedoista ja radioverkon käyttöasteesta. WCS:n karttatyökalu mahdollistaa WLAN-verkkojen suunnittelun ja toteutuksen. Mahdolliset ohjelmistopäivitykset on päivitettävissä kaikkiin järjestelmässä oleviin laitteisiin yhdestä paikasta WCS:n avulla. WCS voidaan asentaa Windows ja Linux -alustoille. (Cisco Systems 2009a.)

4.2 D-Link

D-Link tekee vasta tuloaan keskitetysti hallittavien WLAN-verkkojen markkinoille. D-Linkin WLAN-kontrollerijärjestelmä käsittää kontrollerin ja lightweight-tukiasemia. Ciscon järjestelmästä poiketen D-Linkin WLAN-kontrolleri on WLAN-kytkin. D-Linkillä ei toistaiseksi ole tarjolla kuin kaksi lightweight-tukiasemamallia, DWL-3500AP ja DWL-8500AP, jotka molemmat on ulkoisilla antenniliittimillä. DWL-3500AP on yhdellä 802.11g radiolla, kun taas DWL-8500AP on kahdella radiolla 802.11g ja a-radiolla. (D-Link Corporation 2009b; D-Link Corporation 2009c.)

D-Linkin WLAN-Kytkin DWS-3024 on 24-porttinen Gigabitin-kytkin, jossa lisäksi kaksi valokuituporttia. Yksi DWS-3024 kytkin tukee 48 tukiasemaa, mutta on laajennettavissa tukemaan 192 tukiasemaa pinoamalla 4 kytkintä. Laite on päivitettävissä tukemaan uusinta langatonta 802.11n-standardia. (D-Link Corporation 2009a.)

D-Linkin käyttämän WLAN-kytkin järjestelmän etuna WLAN-kontrollerijärjestelmään nähden on se, että järjestelmä ei tarvitse erillistä kytkintä. Järjestelmän edut tulevat esiin pienten yritysten käytössä, kun yrityksen työasemat ja muut verkkolaitteet on kytkettävissä samaan kytkimeen. Järjestelmän haittoja kilpailijoihin nähden ovat oman tilastointijärjestelmän puute, tukiasemavaihtoehtojen puute ja MESH-tuen puuttuminen.

4.3 Muut laitevalmistajat

Edellä mainittujen Ciscon ja D-linkin lisäksi WLAN-kontrollerijärjestelmiä tarjoaa mm. Meru Networks, Nortel ja Motorola, joiden järjestelmistä löytyy myös tuki MESH-verkkojen rakentamiseen. Valmistajien WLAN-kontrollerijärjestelmät muistuttavat rakenteeltaan hyvin paljon toisiaan, joten järjestelmiä ei käydä sen tarkemmin läpi vaan katsotaan, mitä vaihtoehdot WLAN-kontrolleri ja WLAN-kytkin järjestelmille sisältävät. WLAN-kontrolleri järjestelmänä tarkastellaan Meru Networksin laitteita ja WLAN-kytkin järjestelmänä Motorolan laitteita.

Motorolan järjestelmä on siis WLAN-kytkin järjestelmä, joka käsittää kontrollerin, tukiasemia ja valinnaisen hallintaohjelmiston. Motorolalta löytyy Ciscon WCS:n kaltainen RF Management System (RFMS) langattomien verkkojenhallinta ohjelmisto. (Motorola 2009a; Motorola 2009b.)

AP650 on 802.11a/b/g-standardien lisäksi uutta 802.11n-standardia tukeva perustukiasema ulkoisilla antenniliittimillä. AP-7131 on 802.11a/b/g-standardeja ja uutta 802.11n-standardia tukeva sisäkäyttöön tarkoitettu tukiasema, josta löytyy tuki MESH-verkoille. AP-5181 on 802.11a/b/g-standardeja tukeva ulkokäyttöön tarkoitettu tukiasema, josta löytyy tuki MESH-verkolle. AP-7181 on 802.11a/b/g-standardeja ja uutta 802.11n-standardia tukeva ulkokäyttöön tarkoitettu tukiasema, josta löytyy tuki MESH-verkolle. (Motorola 2009a; Motorola 2009b.)

RFS4000 Wireless LAN Switch on 6-porttinen WLAN-kytkin, joka tukee 24 tukiasemaa ja 24 WLAN-profiilia. RFS6000 Wireless LAN Switch on 6-48- porttinen WLAN-kytkin, joka tukee 256 tukiasemaa, 32 WLAN-profiilia ja 2 000 käyttäjää kytkintä kohden. RFS7000 Wireless LAN Switch on 64–256-porttinen WLAN-kytkin, joka tukee 1024 tukiasemaa, 256 WLAN-profiilia ja 8 000 käyttäjää. RFS-sarjan WLAN-kontrollerit mahdollistavat kahdentoista kontrollerin clusterin luomisen, jolloin esimerkiksi clusteri RFS7000-kytkimillä tukee yli 12 000 tukiasemaa ja 96 000 käyttäjää, RFS6000 3072 tukiasemaa ja 20 000 käyttäjää ja RFS4000 288 tukiasemaa ja 4 600 käyttäjää. RFS6000 ja 7000 ovat saatavissa zero port mallina joka on oikeastaan WLAN-kotrolleri. (Motorola 2009a; Motorola 2009b.)

Merun järjestelmä on myös WLAN-kontrollerijärjestelmä, joka käsittää kontrollerin ja tukiasemia. Kuten D-Linkin järjestelmä ei Merun järjestelmäkään sisällä vielä ainakaan toistaiseksi hallinta-palvelin-sovellusta.

AP150 Series -tukiasemat on 802.11a/b/g-standardeja tukevia ulkoisilla antenniliittimillä varustettuja sisätukiasemia. AP200 Series -tukiasemat on 802.11a/b/g-standardeja tukevia ulkoisilla antenniliittimillä varustettuja sisätukiasemia, jossa on tuki myös MESH-verkoille. AP300 Series -tukiasemat on 802.11a/b/g-standardeja ja uutta 802.11n-standardia tukevia ulkoisilla antenniliittimillä varustettuja sisätukiasemia. OAP180-tukiasemat on 802.11a/b/g-standardeja tukevia ulkokäyttöön tarkoitettuja tukiasemia. (Meru Networks 2008b.)

MC1500-kontrolleri, joka on tarkoitettu pieniin järjestelmiin, tukee 30 tukiasemaan asti ja 500:aa käyttäjää. MC3000 kontrolleri, joka on tarkoitettu keskisuuriin järjestelmiin, tukee 150 tukiasemaan asti. MC4100-kontrolleri, joka on tarkoitettu suuriin järjestelmiin, tukee 300 tukiasemaan asti ja 3 000 käyttäjää. MC5000 on kontrolleri, joka on tarkoitettu jo hyvinkin suuriin järjestelmiin, tukee modulaarisuutensa ansiosta jopa 1 500 tukiasemaa. (Meru Networks 2008b.)

Vaikka valmistajien järjestelmät ja laitteet eroavat toisistaan. Pääsääntöisesti voi todeta, että valmistajilta löytyy kontrollereita niin pieniin muutaman kymmenen tukiaseman kuin suuriin yli tuhannen tukiaseman järjestelmiin. Valmistajat tarjoavat tukiasemia niin sisäkäyttöön kuin ulkokäyttöönkin sekä uusinta 802.11n-standardia tukevia tukiasemia. Cisco ja Motorola tarjoavat myös erillistä hallinta-sovellusta, jonka voidaan olettaa löytyvään muutaman vuoden kuluttua muidenkin järjestelmistä. Tiedot eri valmistajien järjestelmien laitteista ja niiden ominaisuuksista on kerätty valmistajien kotisivuilta löytyvistä esitteistä ja manuaaleista.

5 TOTEUTETUT TESTIYMPÄRISTÖT

5.1 Testiympäristön kuvaus

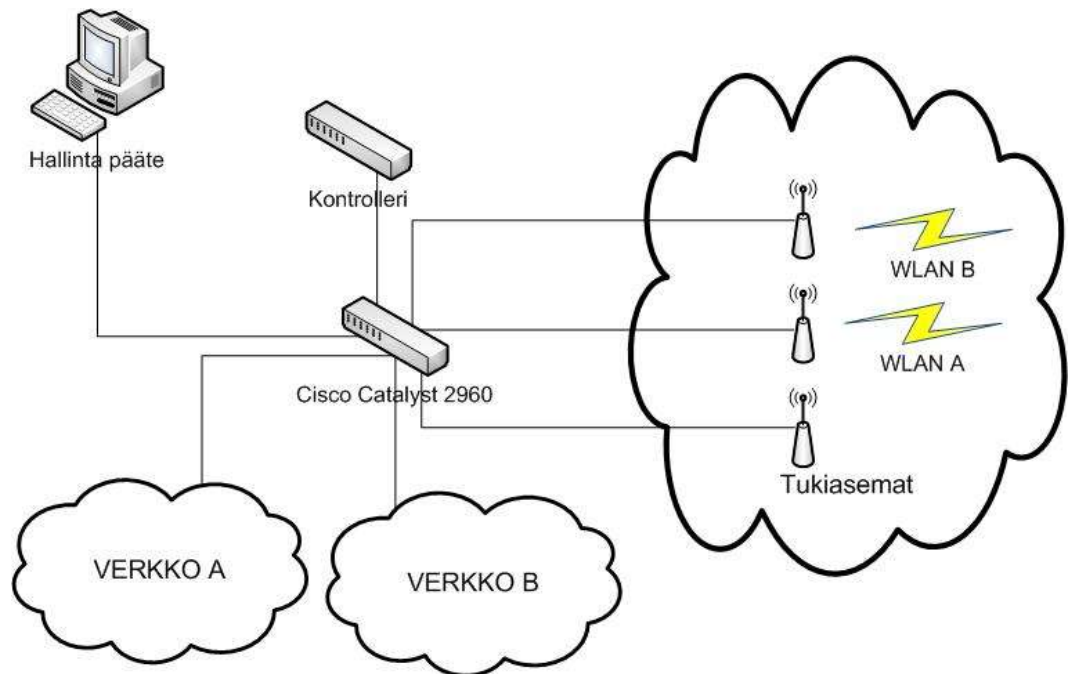
Mastonet-verkon ylläpidon siirtyessä Lahden ammattikorkeakoululle oli tullut ajankohtaiseksi uusia vanhentunutta jo museoiän saavuttanutta laitteistoa ja laajentaa verkon kuuluvuusaluetta HotSpot-periaatteella. Koska verkkoa tultaisiin tulevaisuudessa käyttämään opetusympäristönä, puoltaa sekin seikka laitekannan uusimista ajanmukaisiin laitteisiin, joihin opiskelijat saattavat törmätä myös työelämässä.

Uuden laitteistotoimittajan valinta aloitettiin tutustumalla eri valmistajien keskittyn hallinnan WLAN-ratkaisuihin ja tutkimalla, mikä niistä soveltuisi parhaiten Mastonet-verkkoon. Markkinoilla olevien laitteistojen kartoituksen jälkeen kysyttiin muutamalta valmistajalta mahdollisuutta saada laitteisto koekäyttöön helpottamaan lopullista laitteistotoimittajan valintaa.

Testattaviksi ympäristöiksi valikoituivat markkinajohtaja Ciscon kontrolleriympäristö ja D-Linkin markkinoilla haastajan asemassa oleva WLAN-kytkin ympäristö. Ciscon testiympäristössä kokeiltiin ja tutustuttiin myös MESH-verkon toimintaan. Saatiin myös mahdollisuus ottaa hallintayhteys Meru Networksin laitehuoneessa olevaan kontrolleriympäristöön, jossa konfigurointirajoitusten vuoksi voitiin vain tutkia, miten Merun hallinta eroaa Ciscon ja D-linkin ympäristöistä.

Testien pääpaino oli siis Ciscon ja D-linkin järjestelmien välillä, kuten miten käyttöönotto eroaa toisistaan, mitä статистиikkatietoja on mahdollista saada järjestelmästä ulos ja mitä ominaisuuksia saadaan enemmän Ciscon kalliimmalla hinnalla verrattuna D-linkin halvempaan hintaan. Testiympäristöjen toteutuksen yhteydessä tutkittiin, onko mahdollista luoda järjestelmä, jossa on kaksi erillistä WLAN SSID:tä, joista toinen on suojaamaton WLAN-verkko ja toinen suojattu WLAN-verkko, jollainen järjestely saattaa tulla tarpeelliseksi tulevaisuudessa. Testiympäristöt toteutettiin kuvion 2 esittämän verkkokuvan mukaan, jossa Hallintapäätte ja Cisco Catalyst 2960 -kytkin kuvaavat verkkoinfraa. Kontrollerin ja tukiasemien tilalle sijoitettiin sen järjestelmän laitteet, jota kulloinkin testattiin. Testiympäris-

töissä tukiasemat olivat omassa IP-aliverkossa kiinteillä IP-osoitteilla. Verkoissa oli käytössä kolme erillistä VLANia. Yksi VLAN varattiin tukiasemien ja kontrollerin väliselle CAPWAP- ja LWAPP-liikenteelle ja lisäksi verkot A ja B oli jaettu omiin VLANeihin joissa oli myös omat aliverkot käytössä. Hallintapääteessä oli WindowsXP -käyttöjärjestelmä, jossa oli Mozilla Firefox ja Internet Explorer -selaimet sekä VirtualPC-ohjelma. Testiympäristössä oli myös käytössä virtualisoitu Windows 2003 -serveri, jota pyöritettiin hallinta pääteessä olleella VirtualPC-ohjelmalla. Windows 2003 -serveriä käytettiin DHCP-palvelimena jakamaan IP-osoitteita verkkoon B ja Cison järjestelmää testattaessa WCS-palvelun alustana.



KUVIO 2. Periaatekuva toteutetuista testiympäristöistä

5.2 Cisco-ympäristö

Ciscon järjestelmän testaaminen toteutettiin käytännössä kahdella eri laitteistokoonpanolla. Ensin järjestelmän käyttöönottoa ja peruskäyttöä testattiin koulun harjoituskäytössä olevalla 2100-sarjan kontrollerilla ja parilla 1230-sarja WLAN-tukiasemalla. Cisco toimitti lisäksi testattavaksi ympäristön, joka koostui 2100-sarjan kontrollerista, kolmesta 1520-sarjan WLAN-tukiasemasta ja 1240-sarjan WLAN-tukiasemasta. Molemmissa näissä testiympäristöissä käytettiin myös WCS-palvelimen versiota 5.2.148.0.

Vaikkakin tuotantokäyttöön tuleva kontrollerivalinnan kohdistuessa Ciscon laitteistoon tulisi olemaan 4400-sarjan tuote, toteutettiin testiympäristöt käyttäen 2100-sarjan kontrolleria. Erona 2100- ja 4400-sarjan kontrollereilla on lähinnä 4400-sarjan järeämpi rakenne. 2100-sarjan kontrolleriin voidaan kytkeä maksimissaan 25 WLAN-tukiasemaa, ja 4400-sarjan tuotteeseen 12-100 WLAN-tukiasemaa. 4400-sarjalaisissa on kaksi tai neljä gigabitin kuituliitäntää, joihin tukiasemat kytkeytyvät kun taas 2100:ssa on kahdeksan 10/100 Mb:n RJ45-liitäntää. 1520-sarjan WLAN-tukiasema on MESH-tukiasemaa, joka mahdollistaa MESH-verkon toteuttamisen. 1230-sarjan WLAN-tukiasema on tavallinen ulkoisilla antennilla oleva tukiasema ja 1240-sarjan tukiasema tämän uudempi versio.

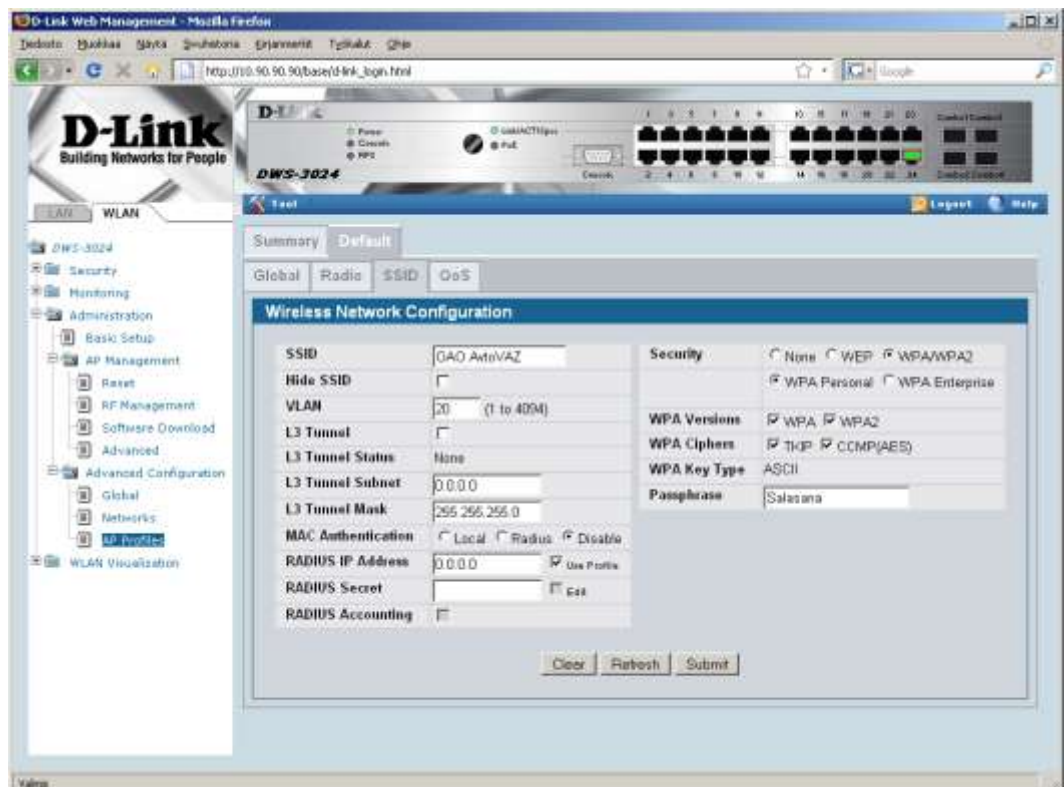
Ciscon testiympäristössä asetetut tavoitteet saavutettiin. Järjestelmä saatiin toimimaan kahdella WLAN-verkolla, joista toinen on salattu ja toinen avoin. Pystyttiin muodostamaan kuva järjestelmän eduista ja haitoista sekä järjestelmän hallinta tuli tutuksi. Testiympäristön käyttöönotto ei tosin onnistunut täysin ilman ongelmia, mutta ongelmat saatiin ratkaistua. Kontrollerin ja kytkimen väliset VLAN-konfiguraatiot olivat suurin ongelma, joka aiheutti muutamaksi päiväksi ohjelmaa, jotta ne saatiin toimimaan halutulla tavalla. Toinen isompi ongelma oli virtuaalikoneen käynnistyessä WCSn sattuman varainen käynnistyminen. WCSn kuutosversioon päivityksen yhteydessä ongelman aiheuttajaksi ilmeni suomen kieliset näppäimistöasetukset.

5.3 D-Link-ympäristö

D-Link toimitti käyttöömmme testiympäristön, joka käsitti DWS-3024 WLAN-kytkimen ja kolme kappaletta DWL-3500-tukiasemaa. D-Linkin järjestelmässä oli tarkoitus tehdä samat testit kuin Ciscon järjestelmässä ja verrata kahden laitteiston eroavaisuuksia. D-Linkin järjestelmän käyttöönotto aloitettiin ottamalla web-hallintayhteys kytkimeen. Web-hallintaan päästään internetselaimella ottamalla HTTP-yhteys (Hypertext Transfer Protocol) osoitteeseen 10.90.90.90, joka on tehdasasetuksilla kytkimen IP-osoite, käyttäjätunnus on admin ja salasanaa ei ole. Web-hallinta avautuu kuvion 3 esittämään näkymään. Sivun yläreunasta voidaan hallita kytkimen porttien ominaisuuksia painamalla hiiren oikeaa näppäintä sen portin päällä ja valitsemalla se ominaisuus pudotusvalikosta, jota haluamme hallita. Kytkimestä nähdään myös aktiiviset portit sekä portit, joissa on PoE (Power over Ethernet) käytössä muuttamalla tämän PoE kohtaan. Kytkimen syvällisempi hallinta on jaettu kahteen osioon, LAN- ja WLAN-osioihin, joista LAN puolella hallitaan kytkimen kytkin ominaisuuksia ja WLAN puolella langattomien verkkojen ominaisuuksia. Kuviossa 4 on esitettyä WLAN-profiilin konfiguraationäkymä.



KUVIO 3. D-Link DWS-3024 WLAN-kykimen hallintanäkymä



KUVIO 4. D-Link WLAN-kykimen WLAN-profiilin konfiguraationäkymä

Ennen kuin tukiasema otetaan hallintaan WLAN-kytkimellä, tarvitsee vaihtaa muutamat tukiaseman asetukset, kuten IP-osoite, koska tehdasasetuksilla tukiasemiin on määritetty kiinteä IP 10.90.90.91, ja jos käytetään VLANeja, tarvitsee muuttaa nämä asetukset myös, jotta tukiasema ja kytkin löytävät toisensa. Tukiaseman konfigurointi tapahtuu web-hallinnan kautta, vaikka konsoliyhteyksinkin on mahdollinen, mutta koska konsoliyhteys otetaan ethernet-portin välityksellä ja tämän samaisen portin asetuksia ollaan säätämässä ja asetukset tulevat saman tien voimaan, niin helposti käy niin, että suljemme itsemme järjestelmän ulkopuolelle. Konsoli on myös vaikeakäyttöinen, vrt. Cisco, joten käytetään web-hallintaa, joka on helpompi käyttöinen ja tehdyt asetukset tulevat buutin yhteydessä vasta voimaan.

Otetaan siis internetselaimella HTTP-yhteys IP-osoitteeseen 10.90.90.91 ja salasana/käyttäjätunnus on admin/admin. IP-osoite vaihdetaan Ethernet Settings -välilehdeltä. Kun käytetään VLANeja, niin asetetaan Management VLAN ID:ksi sama, joka on kytkimen management VLAN sekä Untagged VLAN Disabled -tilaan näin kaikki liikenne liikkuu tagitettuna ja tagittamattomat paketit hylätään. Tukiasemalle voidaan myös kertoa Managed Access Point -välilehdellä osoite, josta hallinta kytkin löytyy, tämä tosin ei ole välttämätön toimenpide. Tämän jälkeen voidaan sulkea web-hallinta ja kytkeä tukiasema WLAN-kytkimeen.

Kuten Ciscon testiympäristössä niin myös D-Linkin testiympäristössä asetetut tavoitteet saavutettiin. Järjestelmä saatiin toimimaan kahdella WLAN-verkolla joista toinen salattu ja toinen avoin. Pystyttiin muodostamaan kuva järjestelmän eduista ja haitoista sekä järjestelmän hallinta tuli tutuksi. Testiympäristön käyttöönoton suurimman ongelman aiheuttivat jälleen VLAN-asetukset, mikä johtui Ciscon ja D-Linkin hieman erilaisesta terminologiasta, joka ratkesi muutaman päivän pohdinnan jälkeen.

5.4 MESH-ympäristö

MESH-verkkoa testattiin jo edellä mainitulla Ciscon toimittamalla testikokoonpanolla, jossa oli siis 2100-sarjan kontrolleri ja kolme 1520-sarjan MESH-tukiasemaa, joista kaksi oli RAP- ja yksi MAP-tukiasema. Testiympäristössä testattiin: miten verkko toipuu vikatilanteista ja verrattiin suorituskykyä tavalliseen tukiasemaan.

Verkko toipui vikatilanteista, kuten RAP-tukiasemalta katkeaa verkkoyhteys tai sähkönsyöttö, odotetunlaisesti. RAP-tukiaseman, jonka kautta MAPin liikenne reititetään virtakatkon jälkeen verkko reititti liikenteen lähes välittömästi uudelleen toisen RAP-tukiaseman kautta kulkevaksi. Verkkoyhteyden katkettua RAP-tukiasemalta, jonka kautta MAP-tukiaseman liikenne kulkee, merkitsi pitempää ja selvästi huomattavaa viivettä uudelleen reitityksessä.

Taulukossa 1 on esitettyä MESH-tukiaseman suorituskyky verrattuna tavalliseen lightweight WLAN -tukiasemaan. Suorituskykyvertailu tehtiin siirtämällä verkon läpi n. 600 Mb CD-levyn kuvatiedostoa ja mittaamalla siirtoon käytetty aika. Saa-dut tulokset ilmoitetaan minuutteina ja sekunteina. RAP- ja WLAN-tukiaseman välillä havaitaan hiuksenhieno ero, joka on luokkaa 30–60 sekuntia, joka selittyy-nee WLAN-tukiaseman yksinkertaisemmalla toiminnalla. MAP-tukiaseman kaut-ta siirrettäessä havaitaan, että liikenne on selvästi hitaampaa kuin vertailu-tukiasemissa, mikä johtuu pelkästään langattomasta hypystä MAP- ja RAP- tukiasemien välillä.

TAULUKOKO 1. MESH-tukiasemien suorituskyky verrattuna tavalliseen WLAN-tukiasemaan

RAP-tukiasema	MAP-tukiasema	1240-sarjan WLAN tukiasema
8 min 06 s	13 min 45s	7 min 06 s
8 min 07 s	10 min 46 s	7 min 35 s

Taulukossa 2 on esitetty, miten tukiasemien ja clientin välisten etäisyyksien kasvaminen vaikuttaa MESH-verkon suorituskykyyn siirrettäessä jo edellä mainittua 600 Mb CD-levyn kuvatiedostoa. Kaksi viimeisintä mittausta vastaa toden mukaisinta tilannetta. Taulukoista 1 ja 2 voidaan todeta, että MESH-verkko on selvästi tavallista WLANia hitaampi ja hyppyjen lisääntyessä hitaus tulisi vielä korostumaan.

TAULUKKO 2. MESH-verkon suorituskyky muutos etäisyyksien kasvaessa

MAP ja RAP lähellä toisiaan	MAP ja RAP etäisyys suurempi	MAP ja RAP etäisyys suuri
MAP ja client lähellä	MAP ja client etäisyys suurempi	MAP ja client etäisyys suuri
9 min 19 s	12 min 10 s	15 min 57 s
9 min 50 s	12 min 35 s	12 min 50 s

5.5 MESH ja WLAN -ympäristöjen vertailu

Kontrolleria ei voida laskea MESHin eduksi WLAN-verkkoon nähden, koska kontrolleriratkaisut tekevät tuloaan myös perinteiseen WLAN-verkkoon. MESHin tavoite on laajentaa olemassa olevien WLAN-standardien ominaisuuksia, kuten saumaton ja katkeamaton langaton verkkoyhteys ilmaitse, reititys, tietoturva, paikannus ja verkkoyhteydet alueille, jonne kaapelointia ei kannata toteuttaa.

Tosin perinteiselläkin WLAN-ratkaisulla voidaan toteuttaa verkkoyhteydet alueille, joille kaapelointi ei kannata, mutta ei yhtä näppärästi kuin MESH:llä. Perinteisessä ratkaisussa jokainen hyppy käsitellään omana kokonaisuutenaan eikä linkkiä ole mahdollista hallita kontrollerista eli linkin kumpaankin päähän tarvitsee käsin konfiguroida tukiasema linkkiä varten. Kahta viiva kolmea linkkiä useampaa ei kannata tehdä perinteisin WLAN-ratkaisuin, vaan tulee aiheelliseksi miettiä MESH-verkkoa tai verkkokaapelointia linkkien tilalle. Perinteisen WLAN-verkon eduksi MESH-verkkoon nähden voidaan laskea toteutuksen huomattavasti huokeampi hinta ja olemassa olevat viralliset standardit.

MESH kärsii vielä tällä hetkellä uuden tekniikan tuomasta ns. ”uutuuslisästä” hinnassaan. MESH:n jokainen hyppy hidastaa tiedonsiirtonopeutta, tästä muodostuu ongelma, kun saman solun sisällä useampi käyttäjä yrittää siirtää suurta tietomäärä. Yhteyden rajoittavaksi tekijäksi muodostuu MESH-runkoyhteys, johon käytetään tällä hetkellä a-standardia, mistä seuraa se, että MESH ei ole vielä oikea vaihtoehto langallisille runkoyhteyksille pysyvämpi luonteisissa ratkaisuisissa. MESH ei ole varteenotettava vaihtoehto, kuin käytössä olevissa satamissa, joissa ei ole mahdollista pysäyttää toimintoja verkko yhteyden kaivuun ajaksi. Tilanne korjaantuu, kun kuitunopeuksiin kykenevät standardit valmistuvat ja ne tulevat MESH-runkoyhteydeksi korvaamaan a-standardia.

MESH on tällä hetkellä jo varteen otettava vaihtoehto langalliselle runkoyhteydelle kohteissa, joissa langaton verkko on tilapäinen ratkaisu. MESH-verkon käyttöä kohteessa tarvitsee todella miettiä siirrettävän datamäärän tarpeen mukaan; jos tarvittava siirtokaista on suuri, tulee langalliset runkoyhteydet edullisemmiksi.

5.6 Testitulokset

Testin perustella tehtiin muutamia huomioita järjestelmistä ja niiden eroavaisuudesta. Ciscon järjestelmän hallinta ja käyttöönotto on vaikeampi kuin D-Linkin, myös logiikaltaan Cisco on vaikeampiselkonen, kuin D-Link. Ciscon järjestelmässä ovat statistiikat huomattavasti paremmat kuin D-Linkissä.

Merun järjestelmän käyttöönottoa ei päästy kokeilemaan testiympäristössä. Etähallintayhteyden välityksellä pääsi vain tutkailemaan Merun järjestelmää, sillä konfigurointimahdollisuuksia rajoitti etäyhteyden käyttö. Meru asettuu D-Linkin Ciscon järjestelmien välimaastoon statistiikat paremmat kuin D-linkissä, mutta ei aivan samaa tasoa kuin Ciscossa. Merun hallintalogiikasta ei voi aivan varmasti sanoa, kun laitteet eivät olleet fyysisesti paikan päällä. Merun hallinnasta täytyi tyytyä katselemaan, mitä voidaan tehdä ja miten se tehtäisiin. Etänä ei viitsinyt konfiguroida liityntää, jossa itse oli kiinne. Merun kontrollerista jäi sellainen vaikutelma, että hallinta oli selkeydessään D-Linkin tasoa, mutta ei aivan yhtä simpeliä ja selkeää, mutta toisaalta hyvin paljon Ciscoa selkeämpi.

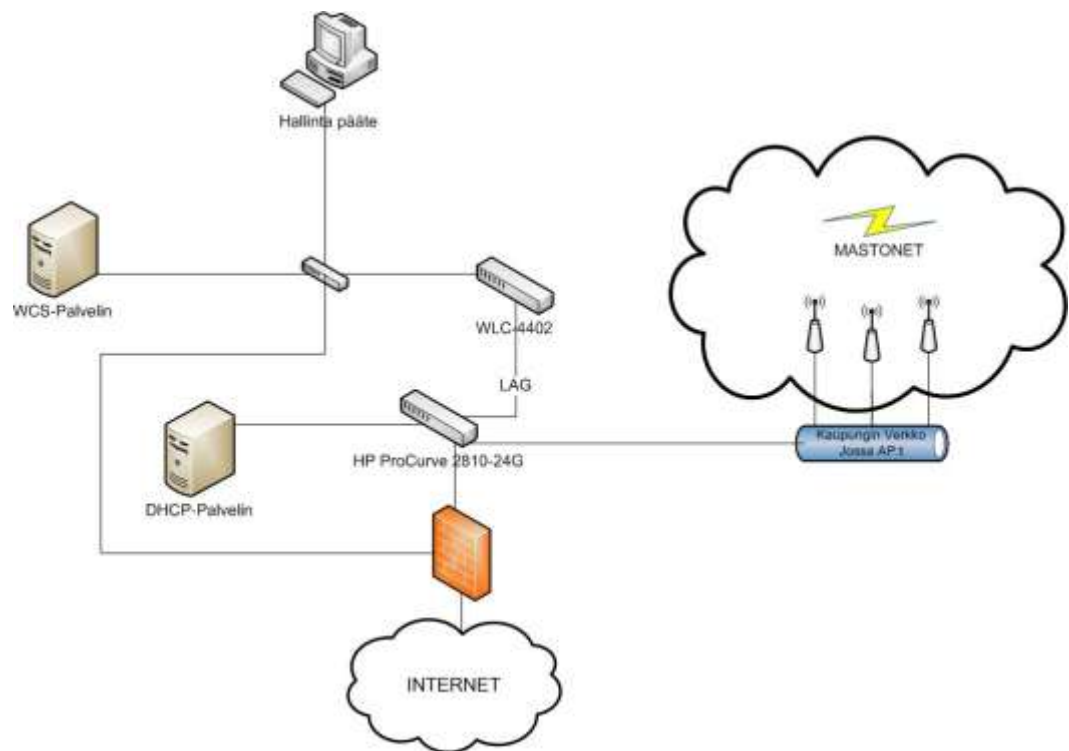
Ominaisuuksiltaan kaikki kolme vaikuttavat olevan hyvin samankaltaisia. Melkein kaikki samat tarpeelliset ominaisuudet löytyivät, kuten esimerkiksi radius-palvelinmahdollisuus. Statistiikka puolelta Cisco oli selvä ykkönen; sen kontrollerista löytyi selkeät ja kattavat statistiikat itsestään, ja siihen kun lisää WCS-palvelimen kylkeen statistiikasta löytyy kaikki tarvittava, Kun taas D-Link, jossa itsessään ei löytynyt kuin liikennemäärät numeroarvoina, oli statistiikoissa kaikkein huonoin, mutta kyllä on tulossa WCS:n kaltainen ohjelmisto, jolla saataisiin kattavammat statistiikat tosin kyllä Cactin ja Zenossin kaltaisilla työkaluilla saataisiin siitäkkin nyt jo varsin kattavat statistiikat. Merun statistiikat asettuvat kahden edellisen välimaastoon statistiikat kyllä oli mutta paljon vaikeammin tulkittavissa kuin Ciscon kontrollerista löytyvät.

Lopullinen järjestelmän valinta tapahtui Ciscon ja D-linkin välillä: valitako halvempi ja jossain määrin vielä puutteellinen järjestelmä vai hinnakkaampi lähes täydellinen järjestelmä. Lopulta vaalinta kohdistui Ciscon järjestelmään tärkeimpinä syinä WCS-palvelin ja laitteet olivat ennakkoon tutumpia ja tuntuivat näin turvallisemmalle ratkaisulle. Valinta olisi aivan yhtä hyvin voinut kohdistua D-Linkin järjestelmään, joka uutena tuttavuutena olisi tuonut uuden opetuksellisen näkökulman Ciscon laitteisiin nähden, joita koululla jo ennestään oli Cisco laboratorion takia. WCSn kaltaisen järjestelmän puute oli kuitenkin niin iso miinus D-Linkin järjestelmälle, että valinta ei kohdistunut siihen tällä kertaa, mutta tilanne voi olla aivan toinen muutaman vuoden kuluttua, kun valitaan uutta kontrolleria, kun tällä kertaa valitun kontrollerin tukemat kaikki 50 tukiasemaa on otettu käyttöön.

6 CISCO-JÄRJESTELMÄN KÄYTTÖNOTTO

6.1 Toteutusympäristön kuvaus

Testien ja kilpailutuksen perusteella valitun Ciscon laitteiston käyttöönotto aloitettiin tekemällä käyttöönotto ensin testiympäristössä, koska testeistä poiketen tuotantoympäristöön tulee 2100-sarjan kontrollerin tilalle 4400-sarjan WLC-4402-kontrolleri 50 tukiaseman lisenssillä. Käyttöönottoa päädyttiin kokeilemaan vielä kerran, koska haluttiin varmistaa, onko jokin oleellisesti muuttunut järeämpään kontrolleriin siirryttäessä. Koeympäristössä toimivuuden varmistuttua suunniteltiin toteutettavan ympäristön verkkokuva, joka on esitettyä kuviossa 5.



KUVIO 5. Kuva rakennettavasta Mastonet-verkosta

Kontrolleri tullaan kytkemään molemmista kuituliitännöistään keskuskytkimeen, joksi valikoitui HPn ProCurve -sarjan tuote ProCurve 2810-24G. Kontrollerin ja keskuskytkimen välille otetaan LAG (Link Aggregation) käyttöön. LAG otetaan käyttöön, koska 4400-sarjan kontrolleri tukee hallintaliityntää kohden 48:aa tukiasemaa ja kontrollerimme on lisensoitu 50 tukiasemalle. Näin ei tarvita kahden tukiaseman takia tehdä toista AP-Manager-liityntää kontrolleriin. Keskuskytkimeltä tulee lähtemään yhteydet DHCP-palvelimelle, kaupungin verkkoon, jossa tukiasemat sijaitsevat ja palomuurin taakse ulkomaailmaan. 4400-sarjan kontrollerissa on mahdollisuus ottaa käyttöön service-portti, jonka kautta on mahdollista hallita kontrolleria. Koska tällainen mahdollisuus on, niin se tullaan ottamaan käyttöön tietoturvan lisäämiseksi. Kontrollerin service-portin taakse tullaan sijoittamaan WCS-palvelin. Näin langattoman verkon käyttäjät eivät pääse kiinne WCS-palvelimeen. WCS-palvelin tarvitsee myös yhteyden Internetiin, jotta se voidaan päivittää. Service portin taakse tullaan sijoittamaan myös järjestelmän hallinta päätte.

Varsinainen ympäristön käyttöönotto aloitettiin asentamalla WCS-palvelin ja tämän jälkeen ottamalla kontrolleri käyttöön. Toki käyttöönoton voi tehdä toisessakin järjestyksessä. Ensin ottamalla kontrollerin käyttöön ja liittämällä toimivan kontrollerin WCS-palvelimeen, mutta koska WCS-palvelimen kautta voidaan hallita kontrolleria, aloitettiin järjestelmän käyttöönotto asentamalla WCS-palvelin ensin.

6.2 WCS-palvelimen asennus

Ympäristöönkäyttöön tuleva versio WCS-palvelimesta on sen kuutos version versio 6.0.132.0. WCS-palvelin päädyttiin asentamaan Linux-alustalle, tosin Windows-alustaa myös harkittiin. Testikokoonpanoissa pyöritettiin WCS-palvelinta Windows-alustalla, minkä takia ennen varsinaista asennusta, joka tulisi tapahtumaan RHEL Linux -alustalle, kokeiltiin voiko WCS-palvelimen asentaa RHEL 5 johdannaisiin CentOS 5.x tai Fedora Core 6 -Linux järjestelmiin. Asennus ei onnistunut CentOS 5.x ja Fedora Core 6 -Linux alustoille, vaikka WCS:ää pystyi huijaamaan, että se luulee, että sitä oltaisiin asentamassa RHEL 5 -järjestelmään.

WCS-palvelu ei aseta vaatimuksia, jotka järjestelmässä pitää olla ennen sen asennusta asennettuna, vaan se tuo kaiken tarvitsemansa asennuspaketissa mukanaan. Linuxia asennettaessa kannattaa jättää SELinux- (Security-Enhanced Linux) ja IPv6- ominaisuudet asentamatta, koska niitä ei tarvita ja ne vaikeuttavat WCS-palvelun toimintaan saattamista. Graafista käyttöliittymääkään ei Linuxiin tarvitse WCS-palvelua varten asentaa, mutta asennettavia paketteja valitessa kannattaa valita sellaiset paketit, että järjestelmään saa asennettua uusimmat päivitykset, kuten yum.

Kun RHEL 5.x Linux uusimmilla päivityksillä on asennettuna palvelinrautaan, voidaan aloittaa WCS-palvelimen asennus. Asennettaessa WCS-palvelua Linuxiin tulee olla kirjautuneena root-tunnuksin järjestelmään. Palomuurista on avattava seuraavat portit WCS-palvelua varten:

- HTTP: määritetään asennuksen aikana (oletuksena TCP 80)
- HTTPS: määritetään asennuksen aikana (oletuksena TCP 443)
- 1315
- 1299
- 6789
- 8009
- 8456
- 8005
- 69 (TFTP)
- 21 (FTP)
- 162 (SNMP Trap)
- 8457.

Ennen varsinaisen asennuksen aloitusta kannattaa luoda ftp- ja tftp-kansiot. Näitä ei suositella sijoitettavan WCS:n asennuskansion alle, koska poistettaessa WCS palvelua poistetaan koko kansio, johon WCS on asennettu, ja jos tftp-kansio olisi tässä kansiossa, poistetaan myös järjestelmän backup-tiedostot.

1. Asennuksen aloitus, jos käytetään graafista käyttöliittymää avataan terminaaliikkuna.

2. a) Asennettaessa WCS CD:ltä siirrytään CD-asemakansion, ja hypätään kohdan kolme ohi

b) Kun asennustiedosto on tallennettu koneen levyille, siirrytään kansioon, johon asennustiedosto on tallennettu.
3. Asennus tiedostosto muutetaan suoritettavaksi komennolla: ***chmod +x WCS-STANDARD-K9-6.0.XX.Y.bin*** jossa XX.Y merkitsevät kyseisen julkaisun versio numeroa.
4. Komennolla ***./WCS-STANDARD-K9-6.0.XX.Y.bin*** käynnistetään asennus scripti. Ensinnäkin scripti valmistelee asennusta, jonka jälkeen kysytään vahvistus lisenssiehtoihin.
5. Asennus tarkistaa, onko edellistä versiota WCS:tä asennettu.
6. Valitaan, onko asennus Primary vai Secondary WCS-serveri.
7. Määritellään käytettävät HTTP- ja HTTPS-portit oletuksena 80 ja 443.
8. Määritetään, halutaanko palvelimen HTTP-porttiin tulevat pyynnöt ohjata HTTPS-porttiin.
9. Määritellään Health Monitorin käyttämä portti.
10. Määritellään root-käyttäjän salasana, jonka tulee täyttää seuraavat ehdot:
 - Salasanassa pitää olla vähintään kahdeksan merkkiä.
 - Salasana ei voi sisältää käyttäjä tunnusta oikein tai väärin päin.
 - Salasana ei voi olla Cisco tai cisco.
 - Root salasana ei voi olla public.
 - Salasanassa on käytettävä kolmea neljästä merkkiluokasta isot kirjaimet, pienet kirjaimet, numerot ja erikoismerkit.
11. Määritellään FTP-salasana.
12. Määritellään FTP-tallennuskansio.
13. Määritellään TFTP-tallennuskansio.
14. Valitaan WCS-asennuskansio.
15. Voidaan luoda WCS-pikakäynnistyslinkit.
16. Asennuksen valmistuttua scripti kysyy, käynnistetäänkö WCS. Annetaan lupa käynnistää WCS, ja jos WCS starteded succesfull -ilmoitus tulee, niin asennus on onnistunut.

Asennusohje on tehty versiolle 6.0.132.0. Ennen jonkin muun WCS-palvelun version asennusta on suositeltavaa katsoa kyseisen version release notesista tai configuration guidesta, onko jokin oleellisesti muuttunut, ja toimia sen mukaisesti. Onnistuneen asennuksen jälkeen otetaan selaimella työasemasta https-yhteys WCS-palvelimeen käyttäen palvelimen IP-osoitetta.

6.3 Kontrollerin käyttöönotto

Kontrollerin käyttöönotto aloitetaan ottamalla konsoliyhteys kontrolleriin, kun kontrolleri on tehdasasetuksilla käyttämällä terminaalisovellusta kuten `tera term`. Konfigurointi aloitetaan suorittamalla `setup wizard`, jota kontrolleri automaattisesti ehdottaa. `Setup wizardin` dialogi, jossa määritellään kontrollerin perus asetukset kuten laitteen nimi, järjestelmänvalvojan salasana ja liityntöjen IP:t, on esitettyinä taulukossa 3. Taulukossa 3 on esitettyinä 2100-sarjan kontrollerin `setup wizard`, joka poikkeaa joiltain osilta 4400-sarjan kontrollerin `setup wizardista`.

`Setup wizardissa` aluksi määritetään laitteelle nimi, järjestelmänvalvojan salasana ja 4400-sarjan kontrollereissa voidaan ottaa LAG käyttöön. Seuraavaksi määritellään hallintaliitännät `management` ja `ap-manager` liityntöjen asetukset. Nämä liitännät olisi hyvä sijoittaa samaan aliverkkoon ja VLANiin toiminnan nopeuttamiseksi. Toki hallintaliityntöjen on mahdollista toimia eri aliverkossa ja VLAN:ssa. Lisäksi määritetään portti, johon hallintaliitännät kytketään, jos otetaan LAG käyttöön ei hallintaliitännöille määritetä porttia. 4400-sarjan kontrollereissa, joissa on `service-porttimahdollisuus`, `setup wizard` kysyy, otetaanko portti käyttöön. Kun portti otetaan käyttöön, määritellään portin IP-asetukset. `Service-portti` ei voi olla samassa aliverkossa `management-` ja `ap-manager-porttien` kanssa. Kun liitännät on konfiguroitu, määritellään langattoman verkon asetukset, kuten SSID, sallitaanko staattiset IP:t WLAN-verkoissa, konfiguroidaanko `radius` palvelin, kerrotaan laitteelle maa, jossa WLAN-verkko toimii, otetaanko mitkä WLAN-verkko standardit a, b tai g käyttöön ja käytetäänkö automaattista taajuus suunnittelua. Lopuksi asetetaan järjestelmäaika järjestelmä, voidaan määrittää hakemaan aika asetukset NTP (Network Time Protocol) palvelimelta, jos sellainen on käytettävissä, tai

määrittää manuaalisesti aika. Setup wizardin aikana määritetyt asetukset on jälkeenpäin täysin muutettavissa.

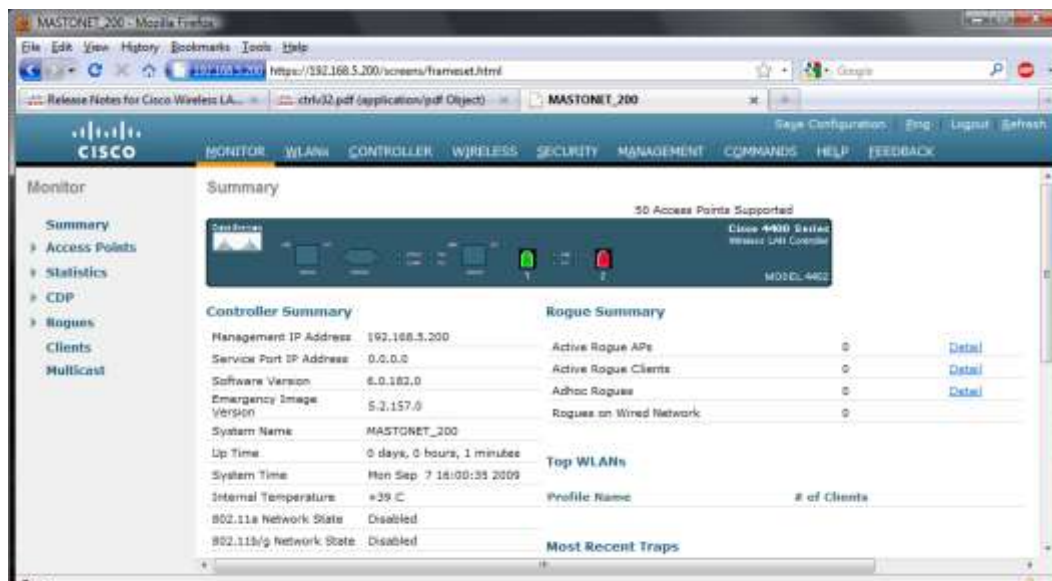
TAULUKKO 3. 2100-sarjan kontrollerin setup wizard -dialogi

System Name [Cisco_cf:ec:60] (31 characters max):Systeemi
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Re-enter Administrative Password : *****
Management Interface IP Address: 10.10.10.10
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 8]: 1
Management Interface DHCP Server IP Address: 10.10.10.10
AP Manager Interface IP Address: 10.10.10.11
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (10.10.10.10):
Virtual Gateway IP Address: 10.10.20.1
Mobility/RF Group Name: Ryhma
Network Name (SSID): Moskvits
Allow Static IP Addresses [YES][no]: no
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code list (enter 'help' for a list of countries) [US]: FI
Global Public Safety State: Already configured, Configuring Local States
Enable 802.11b Network [YES][no]: YES
Enable 802.11a Network [YES][no]: no
Enable 802.11g Network [YES][no]: YES
Enable Auto-RF [YES][no]: YES
Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: YES
Enter the date in MM/DD/YY format: 06/05/09
Enter the time in HH:MM:SS format: 10:00:00
Configuration correct? If yes, system will save it and reset. [yes][NO]:

Mastonet verkkoa varten setup wizardissa määritettiin seuraavat asiat:

- Määritettiin kontrollerille nimi.
- Määritettiin järjestelmänvalvojan salasana.
- Otettiin LAG käyttöön.
- Määritettiin management ja ap-manager liitynnöille IP-osoitteet samasta aliverkosta, johon tukiasemat tullaan sijoittamaan sekä sama VLAN.
- Otettiin service-portti käyttöön ja määritettiin sille IP:t.
- RF-groupiksi ja SSID:ksi määritettiin MASTONET.
- Radiusta ei määritelty.
- Toimintamaaksi asetettiin Suomi FI.
- a-, b-, ja g-verkot otettiin käyttöön automaattisella taajuus suunnittelulla.
- Järjestelmän aika määritettiin manuaalisesti.

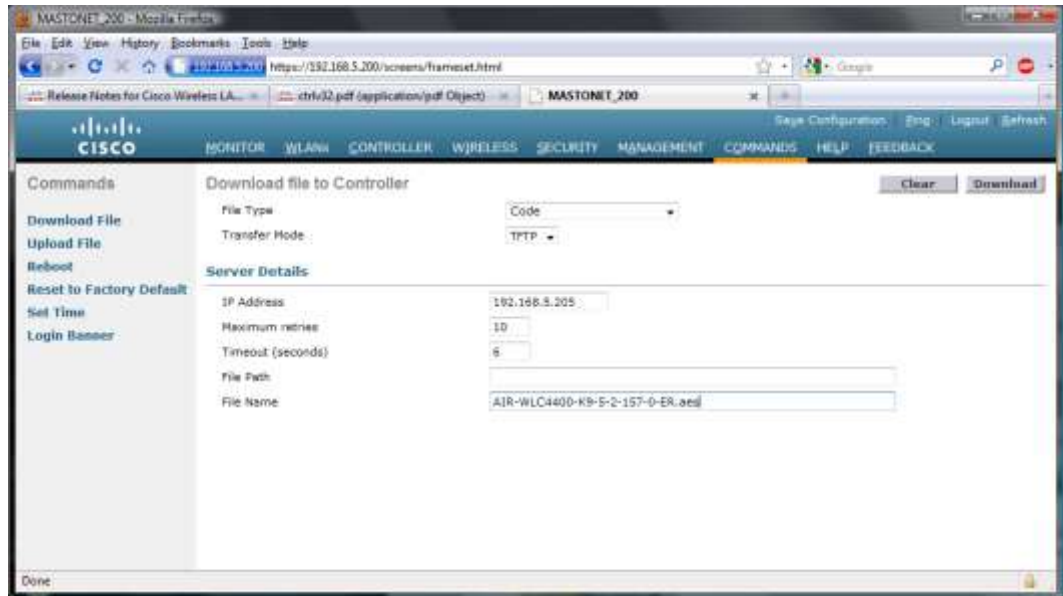
Kontrollerin setup wizardin jälkeen otettiin selaimella yhteys Service-portin IP-osoitteeseen ohjelmiston päivitystä varten, koska tehtaalta tullessa kontrolleri oli varustettu 4-version ohjelmistolla ja haluttiin uusin 6-version ohjelmisto käyttöön. Tässä vaiheessa ei vielä otettu WCS-palvelin yhteyttä vaikkakin varsinaista käyttöönottoa jatkettiin sen kautta. Yhteys suoraan kontrollerin tarvittiin ohjelmisto päivityksen suorittamisen takia, koska ohjelmistoa ei voi päivittää WCS-palvelimen kautta. Kuviossa 6 on esitettyä kontrolleriin sisäänkirjautumisen jälkeen avautuva etusivu.



KUVIO 6. Kontrollerin hallinta näkymä

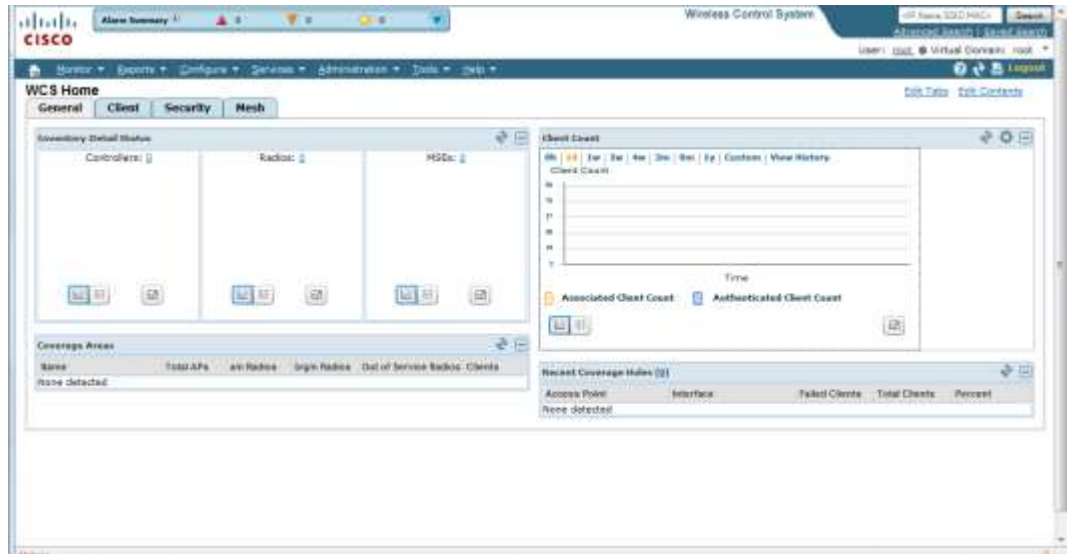
Ohjelmiston päivitys aloitetaan lataamalla Ciscon internetsivustolta uusimman ohjelmiston 6.0.182.0 kooditiedosto AIR-WLC4400-K9-6-0-182-0.aes ja Emergency Imagen tälle AIR-WLC4400-K9-5-2-157-0-ER.aes. Emergency Image ei ole välttämätön, vaan kontrolleri lataa tämän vanhemman ohjelmistoversion siinä tapauksessa, jos pääohjelmisto on vioittunut. Ohjelmakoodit voidaan ladata kontrolleriin joko FTP- (File Transfer Protocol) tai TFTP-protokollaa (Trivial File Transfer Protocol) käyttäen. TFTP on helpompi ja nopeampi käyttää kuin FTP, jos ei ole käytettävissä FTP-palvelinta. TFTP tarvitsee vain TFTP-ohjelmiston työasemaan pyörimään ja siirrettävät tiedostot kopioidaan ohjelmaan määritettyyn TFTP-kansioon. Ennen ohjelmiston päivityksen aloitusta WLAN-verkot tarvitsee disabloida kontrollerista, koska ohjelmisto päivitetään samalla kontrolleriin kytettyihin tukiasemiin, jos WLAN-verkoissa olisi liikennettä hidastuisi päivitys huomattavasti. WLAN-verkon disablonti tapahtuu *WLANs*-valikon *WLANs*-alavalikosta valitsemalla WLAN-verkon profiili. WLAN-verkon profiilin *General*-välilehdellä otetaan täppä pois *status enabled* -ruudusta. Ohjelmiston päivitys aloitetaan valitsemalla *COMMANDS*-valikosta *Download File*. Kuviossa 7 on esitettyä Donload file -näkymä, johon ohjelmistoa päivitettäessä määritetään seuraavat asetukset: File Type on Code, Transfer Mode on TFTP, IP Address on sen laitteen, jossa TFTP-palvelu sijaitsee, IP-osoite ja File Name ohjelmistokoodi tiedoston nimi File Path -asetusta ei tarvitse määrittää jos tiedosto suoraan TFTP

ohjelmaan määritetyn TFTP kansion juuressa. Valitsemalla *Download* kontrolleri alkaa päivittää itseään, ja kun päivitys valmistuu, kontrolleri kysyy käynnistytäänkö uudestaan. Uudelleen käynnistys on pakollinen ennen kuin voidaan ladata Emergency Image, jos sitä käytetään, jotta tehdyt muutokset tulisivat voimaan. Emergency Image ladataan samalla tavalla kuin ohjelmistokoodikin. Ohjelmiston päivityksen jälkeen on muistettava ottaa käyttöön disabloidut WLAN-verkot.



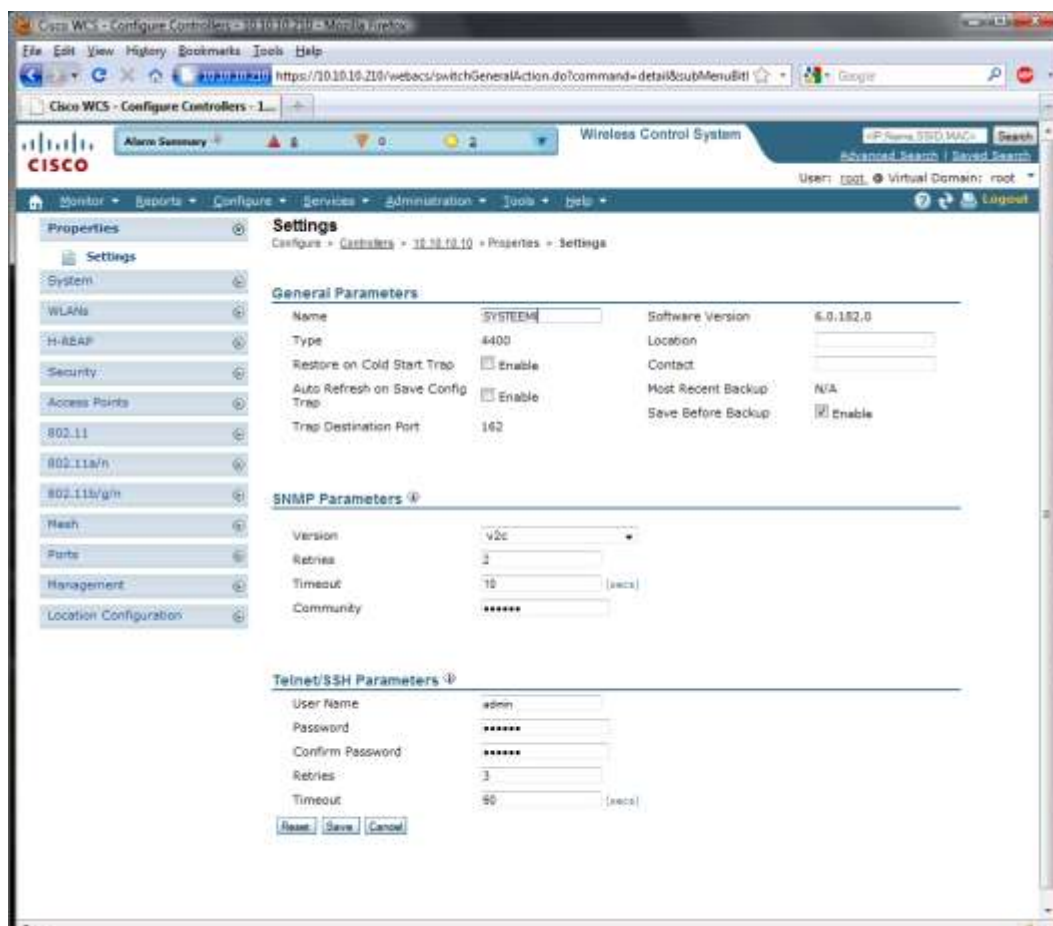
KUVIO 7. Kontrollerin Download file -näkyvä

Kontrollerin päivityksen jälkeen jatkettiin käyttöönottoa ottamalla yhteys WCS-hallintapalvelimeen. Jos WCS-palvelinta ei olisi käytettävissä, yhteys otettaisiin kontrollerin management-liityntään, tai jos käytettävissä on service-portti yhteys, voidaan ottaa service-porttiin. Yhteydenotto tapahtuu internetselaimella https-protokollaa käyttäen. Kuviossa 8 on esitetty sisäänkirjautumisen jälkeen avautuva WCS-hallintapalvelimen etusivu.



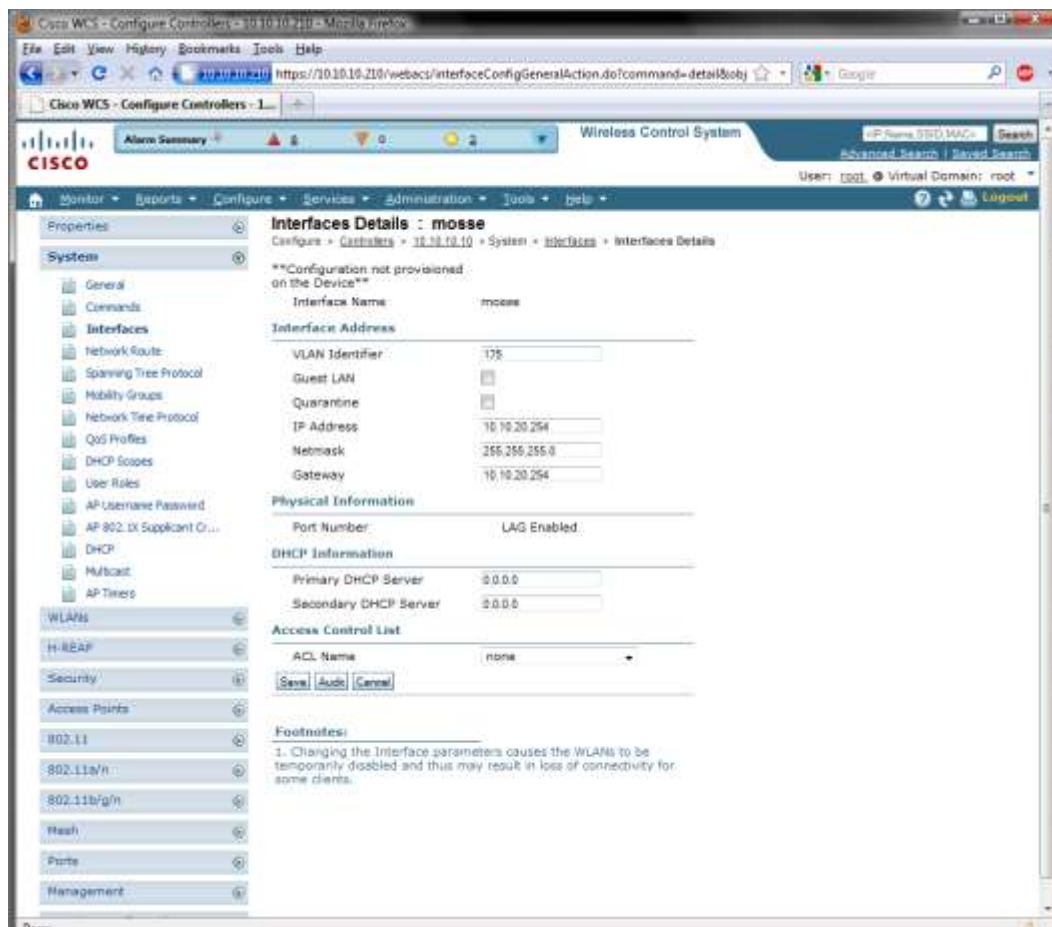
KUVIO 8. WCS-hallintapalvelimen etusivu

WCS-palvelimen hallintayhteyden avauduttua aloitettiin ottamalla kontrolleri hallintaan. Kontrollerin hallintaanottaminen tapahtuu valitsemalla *Configure*-valikosta *Controllers* ja avautuvasta näkymästä valitsemalla oikeassa yläkulmassa sijaitsevasta pudotusvalikosta *Add Controllers...* ja *Go*. Avautuvaan näkymään kirjoitetaan *Ip Addresses* -kenttään kontrollerin service -portin IP-osoite, jos portti on käytettävissä tai management-liittymän IP-osoite ja *User Name* ja *Password* -kenttiin kontrollerin järjestelmänvalvojan käyttäjätunnus ja salasana OK painikkeesta WCS-palvelin yrittää ottaa kontrollerin hallintaansa. Kun kontrolleri on saatu onnistuneesti hallintaan, avautuu kuvion 9 mukainen näkymä, jossa oikeassa reunassa on kontrollerin hallintavalikko.



KUVIO 9. Kontrollerinhallinnan etusivu WCS-palvelimessa

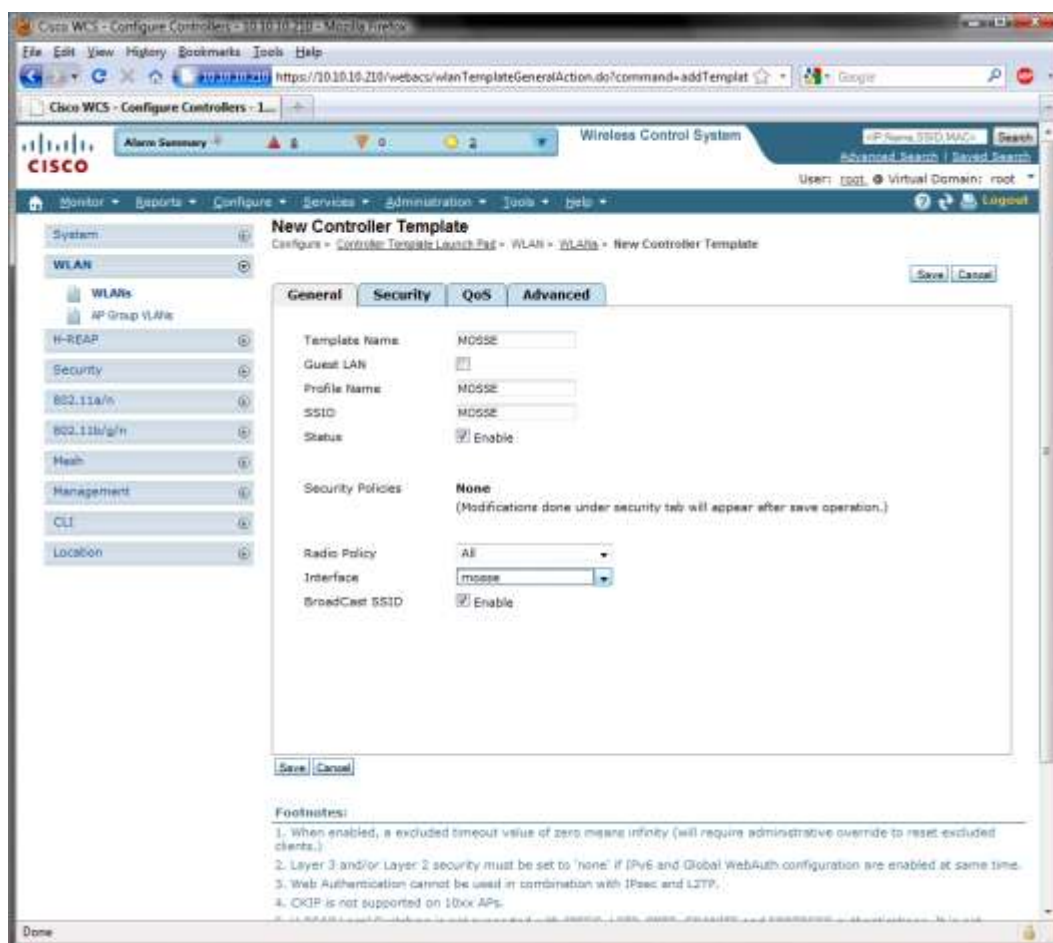
Kontrollerin hallintaan ottamisen jälkeen jatkettiin luomalla WLAN-verkkojen tarvitsemat liittynät, jotta voidaan käyttää VLAN-verkkoja WLAN-verkoille. Liittynnän luominen tapahtuu valitsemalla *System*-valikosta alavalikon *Interfaces* ja avautuvasta näkymästä valitsemalla oikeassa yläkulmassa sijaitsevasta pudotusvalikosta *AddInterface...* ja valitsemalla *Go*. Avautuvassa ikkunassa annettiin liittynnälle nimi. Liityntää nimettäessä liityntä kannattaa nimetä samalla nimellä kuin se WLAN-verkko, mikä liityntään tullaan liittämään. Mastonet-verkon tapauksessa liityntä nimettiin mastonetiksi. Kun liityntä on nimetty, valitaan *OK* ja avautuu kuvion 10 näkymä, jossa määritettiin liittynnän asetukset, kuten IP-osoite ja VLAN. Liittynnän IP-osoite valittiin siten, että liittynnän IP-osoite tuli samaan aliverkkoon, johon WLAN-verkon käyttäjät tulevat liittymään ja VLAN:ksi sellainen, joka ei vielä ollut käytössä verkossa. Kontrolleriin luotiin kaksi tällaista liittyntää, joihin tullaan liittämään WLAN-verkot.



KUVIO 10. Liitynnän konfigurointinäkymä

Liityntöjen luomisen jälkeen jatkettiin langattomien verkkojen luomisella. Kontrolleriin otettiin käyttöön kaksi WLAN-profiilia: toinen Mastonet-verkolle ja toinen WPA2 salattu, jonka käyttötarkoitus tarkentuu myöhemmin verkon tuotanto-käyttöönottamisen jälkeen. Kontrolleriin luotiin jo setup wizardin yhteydessä yksi WLAN-profiili, jota tarvitsi hieman muokata. Tämän lisäksi luotiin toinen avoin WLAN-profiili Mastonet-verkkoa varten.

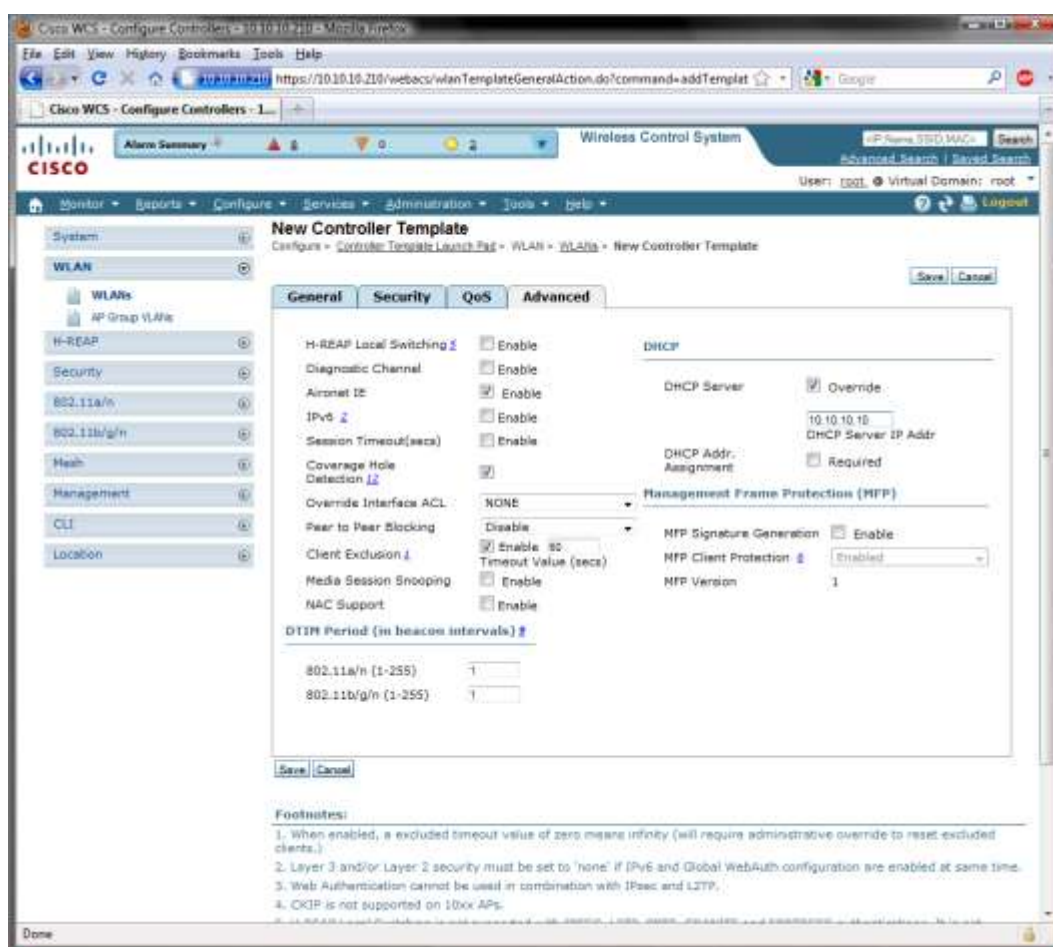
Langattoman verkon luominen tapahtuu valitsemalla *WLANs*-valikosta alavalikon *WLAN Configuration* ja avautuvasta näkymästä valitsemalla oikeassa yläkulmassa sijaitsevasta pudotusvalikosta *AddWlan...* ja valitsemalla *Go*. Avautuu näkymä, jossa WCS ehdottaa WLAN-templaten eli mallin luomista. Malli on pakko luoda, jotta voidaan luoda uusi WLAN-verkko. Yhden kontrollerin verkossa WLAN-malli on sinänsä tarpeeton, mutta useamman kontrollerin verkossa valmis WLAN-malli voidaan tiputtaa verkon jokaiseen kontrolleriin samanlaisena. Mallia tehtäessä kannattaa WLAN-verkko nimetä samalla nimellä kuin liityntä, johon verkko liitetään, sekä SSID. Nimeämisen jälkeen verkko voidaan tallentaa ennen muiden asetusten määrittämistä *Save*-nappulasta. WLAN-profiilin *General*-välilehdellä kuviossa 11 määritetään verkon tila, mitkä radiot verkolla käytössä, liityntä, johon verkko liitetään ja lähetetäänkö SSID. Profiilin *Security* -välilehdeltä muokataan salausasetukset, kuten käytetäänkö web- tai wap-salauksia. Mastonet-verkon tapauksessa jätetään verkko avoimeksi eli valittiin open.



KUVIO 11. WLAN-profiilin konfiguraation General-välilehti

Kuvio 12 WLAN-profiilin advanced-välilehdellä valittiin DHCP-optioksi override ja kerrottiin DHCP-palvelimen IP-osoite, koska palvelin sijaitsee eri aliverkossa kuin liityntä, johon WLAN kytkettiin. Required DHCP -optio joka myös valittiin määrittää WLAN-verkossa sallituiksi IP-osoitteiksi vain DHCP-osoitteet. Mallia luotaessa ensimmäisen tallennuksen jälkeen tulee näkyviin *Apply to Controllers...*-nappula, jota painamalla WCS kysyy, mihin kontrolleriin malli siirretään. Kun kontrolleri on valittu, siirretään malli valittuun kontrolleriin.

Setup wizardia suoritettaessa luotiin toinen WLAN-verkko, jonka salaus asetukset eivät olleet halutunlaiset, vaan salaus muutettiin WPA2-salaukseksi. Salauksen muuttaminen tapahtuu valitsemalla WLAN-profiili listauksesta kyseinen WLAN ja sen security-välilehdeltä muutettiin security asetukset: WPA2, PSK (Pre Shared Key) ja annettiin WPA2 salasana. Lopuksi liitettiin General-välilehdeltä toiseen aiemmin luomaamme liittymään muttamalla Interface-asetusta.

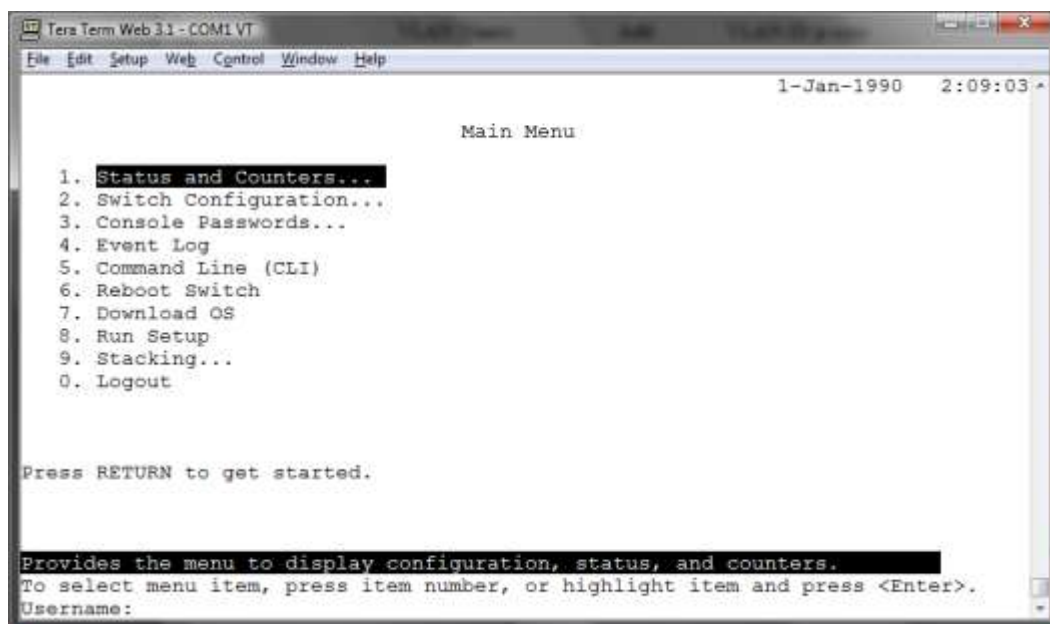


KUVIO 12. WLAN-profiilin konfiguraation Advanced-välilehti

6.4 Tukiasemien liittäminen kotrolleriin

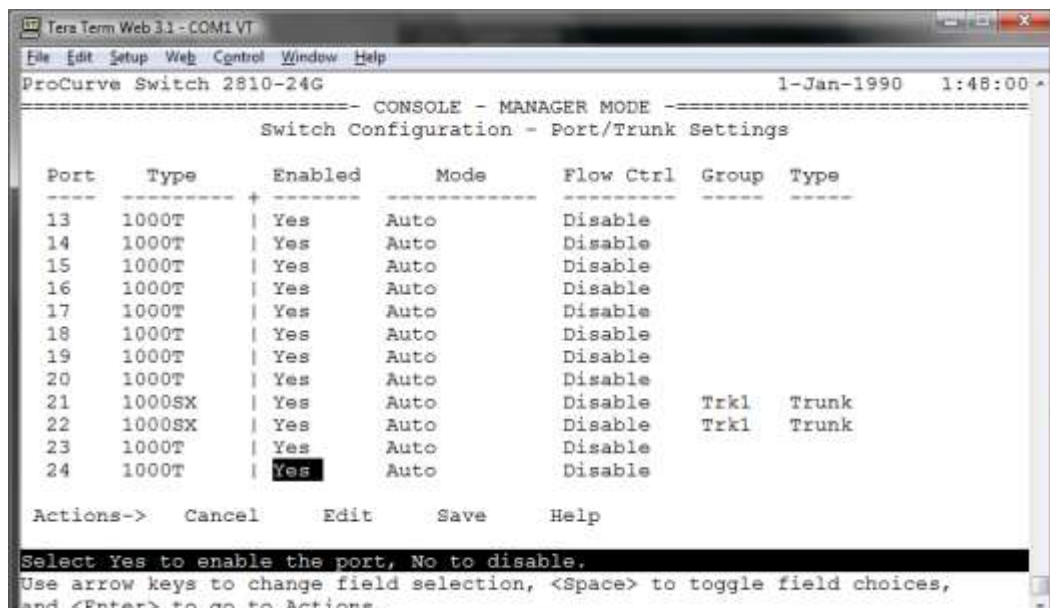
Ennen kuin tukiasemat voidaan liittää kontrolleriin, tarvitsee HP ProCurve 2810-24AG -kytkin konfiguroida. Kytkimen voi konfiguroida käyttämällä komentoriiviä, menuvalikkoa tai web-liityntää. Kytkimen konfigurointi suoritettiin menuvalikon avulla, on konfigurointi helpompaa kuin komentoriviltä suoritettuna. Menuvalikkoa käytettäessä ei tarvita asettaa IP-osoitetta web-liityntää varten. Konfigurointi aloitetaan ottamalla konsoliyhteys kytkimeen esimerkiksi Tera Term -sovelluksella. Avautuvalle komentoriville kirjottamalla menu pääsee menuvalikkoon, joka on esitettyä kuviossa 13.

ProCurve Switch 2810-24G# menu



KUVIO 13. HP ProCurve -kytkimen menuvalikko

Kytkimen konfigurointi aloitetaan *Switch Configuration...* -valikosta. Ensin konfiguroitiin kytkimen portit, jotka tulevat kiinne kontrolleriin Trunk-tilaan, jolloin kuorma tasataan porttien välillä ja yhteydestä tulee vikasietoisempi. Trunk-tilaan portit kyketään valitsemalla *Port/Trunk Settings* avautuu kuvion 14 näkymä. Edistillä pääsee konfiguroimaan portteja. Porteille, jotka on kytketty kontrollerin kuituliityntöihin, asetetaan Goupiiksi Trk1 ja Typeksi Trunk. Tyypiksi ei pidä asettaa LACP (Link Aggregation Control Protocol), koska Ciscon LAG ei ole LACP-protokollan mukainen.



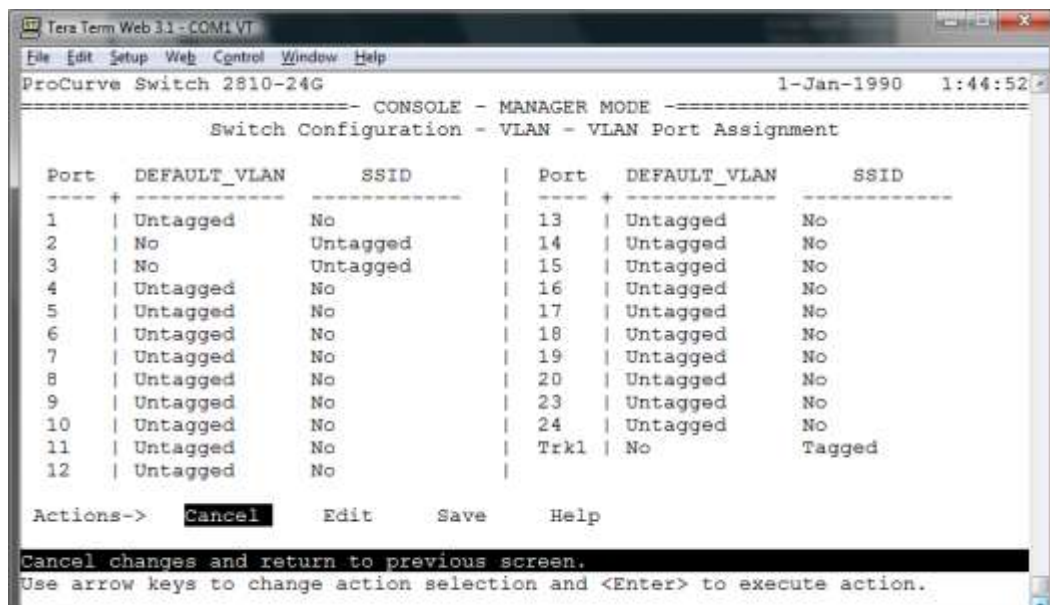
Port	Type	Enabled	Mode	Flow Ctrl	Group	Type
13	1000T	Yes	Auto	Disable		
14	1000T	Yes	Auto	Disable		
15	1000T	Yes	Auto	Disable		
16	1000T	Yes	Auto	Disable		
17	1000T	Yes	Auto	Disable		
18	1000T	Yes	Auto	Disable		
19	1000T	Yes	Auto	Disable		
20	1000T	Yes	Auto	Disable		
21	1000SX	Yes	Auto	Disable	Trk1	Trunk
22	1000SX	Yes	Auto	Disable	Trk1	Trunk
23	1000T	Yes	Auto	Disable		
24	1000T	Yes	Auto	Disable		

Actions-> Cancel Edit Save Help

Select Yes to enable the port, No to disable.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.

KUVIO 14. HP:n ProCurve-kytkimen portti konfiguraatio näkymä

Kun portit on luotu, konfiguroidaan vielä VLAN asetukset. VLAN-asetukset konfiguroidaan *Switch Configuration...* -valikosta valitsemalla *VLAN Menu...* -valikko. *VLAN Names* -valikossa nähdään, mitä VLANeja kykimeen on konfiguroitu, ja luodaan uusia VLANeja valitsemalla *Add VLAN*. VLANeja luodaan sama määrä kuin kontrolleriin luotiin ja VLAN ID:ksi annetaan samat, mitä kontrollerin konfiguroitiin. VLANit kannattaa nimetä selkeästi. VLANien luomisen jälkeen ne tarvitsee vielä asettaa portteihin. VLANien portteihin asettaminen tapahtuu VLAN-Menun *VLAN Port Assigment* -valikosta kuvio 15. VLANit asetetaan siten, että Trk1-porttiin asetetaan tagitettuna kaikki kontrolleri järjestelmän VLANit. Muut portit asetetaan Untagged tilan. Tukiasemilla Untaggedina vain kontrollerin management VLAN ja WLAN-verkkojen VLANit Untaggedina siihen porttiin, josta löytyvät. Muihin kuin Trk1-porttiin asetetaan VLANit Tagged tilaan vain, jos porttiin tulee useampi VLAN. Lopuksi voidaan tarvittaessa käydä määrittämässä IP-asetukset disabled tilaan näin kytkimellä ei ole IP-osoitetta ja on hallittavissa pelkästään konsoli-portin välityksellä. IP:t disabloidaan *Switch Configuration...* -valikosta löytyvästä *IP Configuration* -valikosta. Asetetaan vielä salasana suojaus kykimelle ja kytkin on valmis käyttöön otettavaksi.



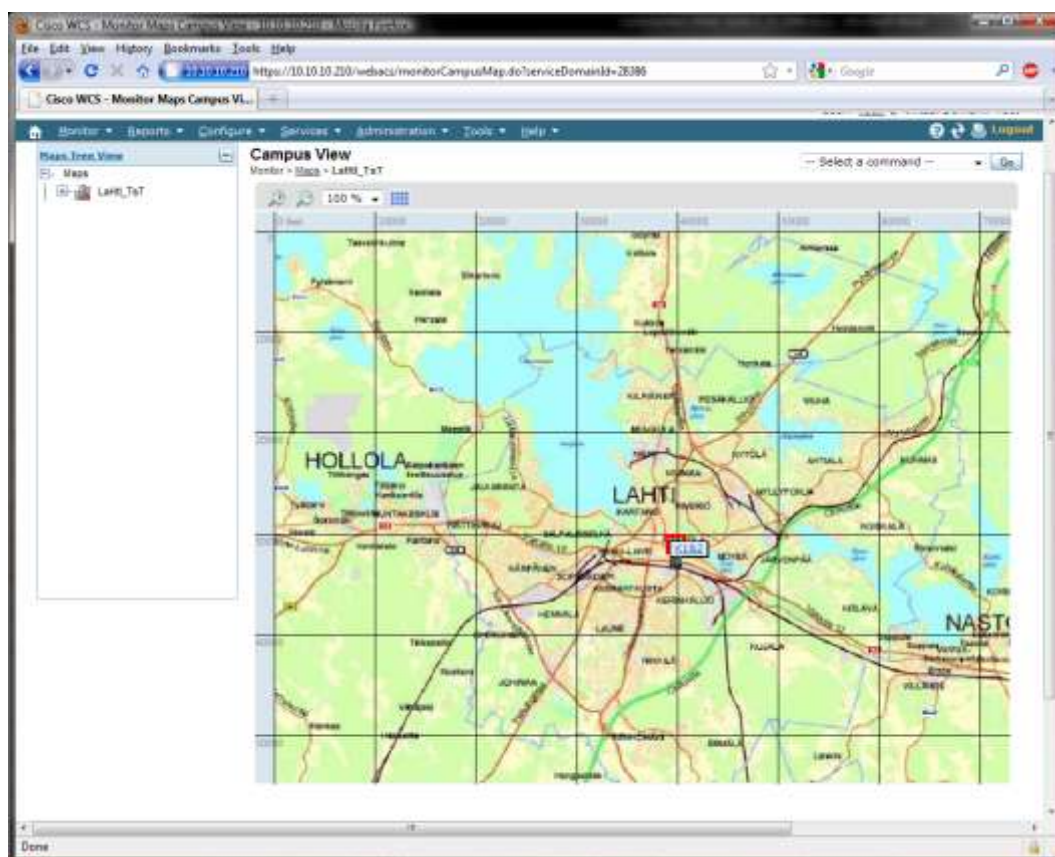
KUVIO 15. VLAN Port Assigment -valikko

Tukiasema kytkeytyy kontrolleriin CAPWAP-protokolla käyttäen, ja kaikki liikenne tukiaseman ja kontrollerin välillä kulkee CAPWAP-tunnelissa. Tukiasemille jaetaan staattiset DHCP -osoitteet eli tukiasema saa buutin jälkeen aina saman IP-osoitteen DHCP-palvelimelta. Staattista DHCP:tä käytettäessä tiedetään buutinkin jälkeenkin, missä tukiasema sijaitsee. Jos käytettäisiin dynaamista DHCP:tä, tukiaseman IP voisi vaihtua buutin jälkeen. Tukiasemia ei voi nimetä, vaan tukiaseman tunnistaminen tapahtuu MAC- tai IP-osoitteen avulla. IP-osoite on yksinkertaisempi tapa tunnistaa tukiasema kuin MAC-osoite, minkä takia käytetään staattisia IP:tä. Staattiset IP:t toteutetaan DHCP-palveluna, joka vähentää tukiasemaan tehtävien muutosten määrä, kun tukiaseman IP:tä ei tarvitse muuttaa.

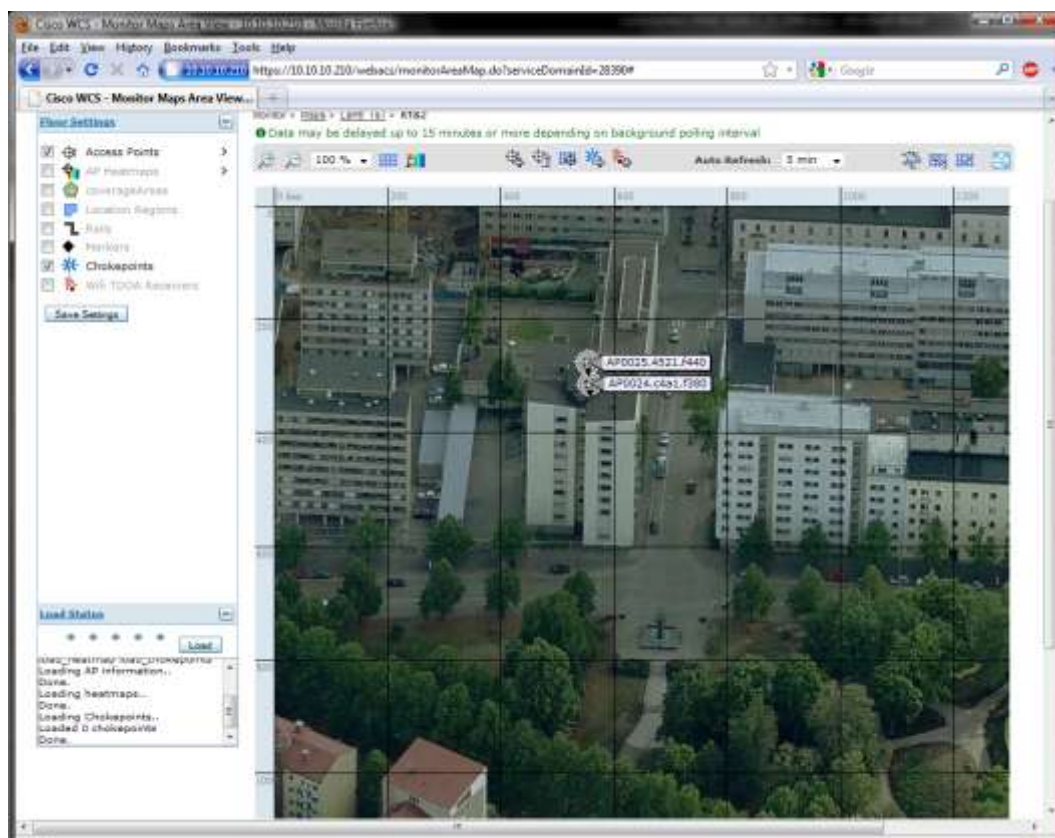
Tukiaseman liittyessä kontrolleriin se saa automaattisesti saman ohjelmistoversion, joka kontrollerilla jo on. Näin tukiasemia ei tarvitse erikseen päivitellä. Kun tukiasemat on liitetty kontrolleriin, on verkko valmis käytettäväksi. Verkon toimivuus todetaan vielä liittymällä WLAN-verkkoon. Kun liittyminen onnistuu ja saadaan IP-osoite oikeasta aliverkosta, niin järjestelmä on valmis käytettäväksi.

6.5 WCS-palvelimen kartta- ja raporttiominaisuudet

Kun järjestelmä on käytössä, WCS-palvelin tarjoaa kartta- ja tilastioominaisuuksia, joilla voidaan valvoa verkkoa. WCS:n karttaominaisuudella voidaan luoda kuuluvuus- ja tukiasemien sijainti karttoja. Kuviossa 16 on esitetty maantieteellinen kartta, johon voidaan merkitä ulkotukiasemien ja rakennusten sijainteja, joissa tukiasemat ovat. Maantieteellisestä kartasta saadaan avautumaan kuvion 17 mukainen näkymä, johon on merkittynä ulkotukiasemien sijainti. Tähän näkymään WCS voi piirtää kuuluvuuskartan. Jos tukiasemat sijaitsevat sisätiloissa, voidaan tehdä rakennus, josta avautuu kerrokset pohjapiirroksina ja näihin piirtyy verkon kuuluvuus karttaväreinä. Kuviossa 16 ja 17 ei ole todellakaan esitettyä ainoa oikea kartta malli, vaan kartta kannattaa luoda kuhunkin järjestelmään sellaisena minkä parhaaksi näkee. Karttaominaisuus mahdollistaa myös verkon etukäteissuunnittelun. Näin ei tarvita erillistä verkon suunnitteluohjelmistoa.

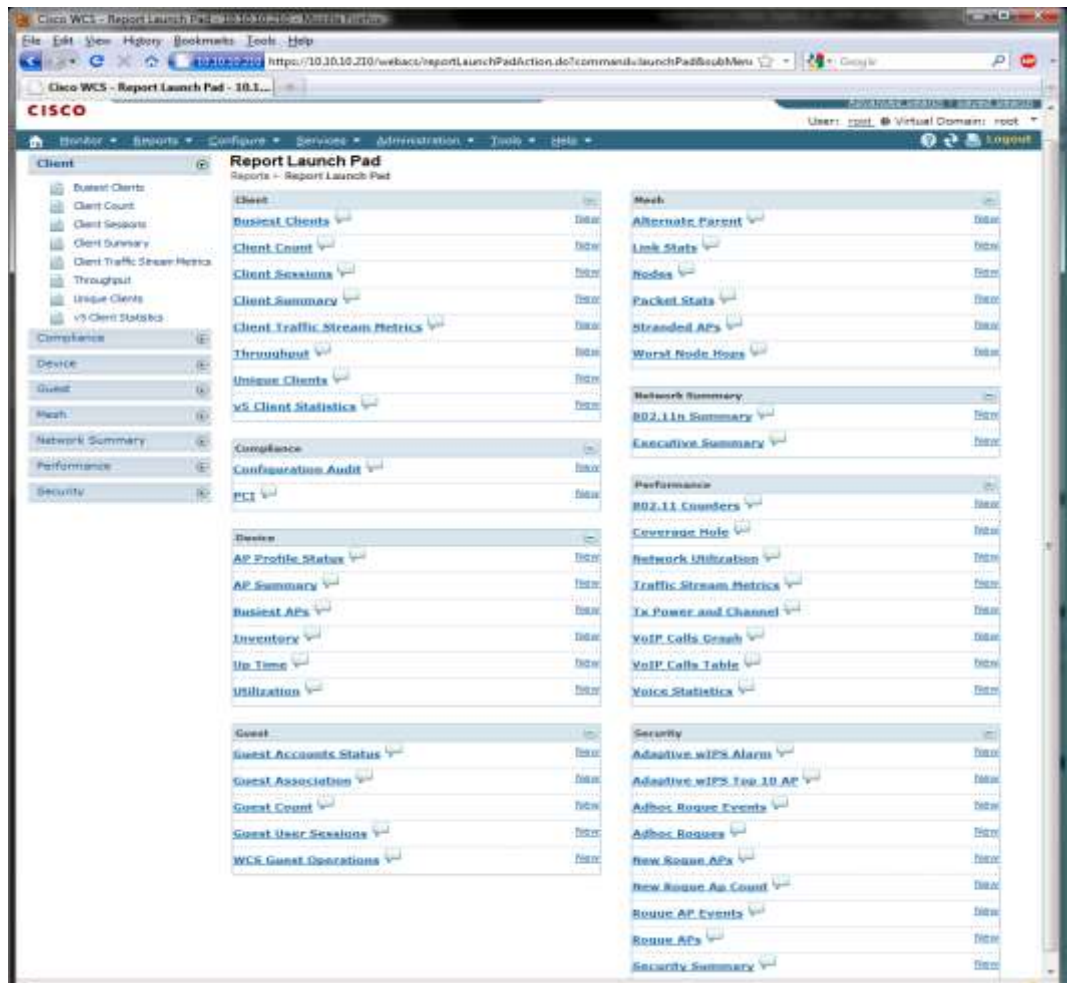


KUVIO 16. WCS-Palvelimen karttatyökalu



KUVIO 17. WCS-palvelimen karttatyökalun rakennusmalli

WCS:n tilastointipalvelut löytyvät *Reports*-valikon *Report Launch Pad* -valikosta. Kuviossa 18 on raportointikeskuksen näkymä, josta löytyy raportointi mahdollisuuksia. Raporteista voi luoda ja tallentaa valmiita malleja, joita ajetaan tarpeen mukaan, tai vaan luoda uuden raportin. Raporttimallin voi määrittää ajastettuna, jolloin WCS luo raportin automaattisesti. Raportteja voidaan luoda mm. liikennemäärästä, yksilöllisistä MAC-osoitteista, naapuritukiasemista ja kiireisimmistä tukiasemasta. Lisäksi MESH-verkkoa voidaan raportoida erikseen. Esimerkki WCS-palvelimen raportista on esitettyä kuviossa 19. Listauksen lisäksi voidaan piirtää kuvaajia. Näissä testiympäristöissä raporttien testaaminen jäi vähäiselle vähäisen tukiasema määrän ja vähäisen käytön takia ei oikein pystynyt luomaan hyviä kuvaavia raportteja. Raporttiominaisuuksia päästään paremmin testaamaan tuotantoympäristössä, kun verkkoon saadaan liikennettä, mitä analysoida.



KUVIO 18. WCS-palvelimen raporttityökalu

Report Run Result

Wireless Control System

Generated: Tue Dec 01 12:18:03 EET 2009

Report By: Controller
 Controller: All Controllers
 Protocol: All Clients
 Reporting Period: Last 84 days

Unique Clients

Start Time	User MAC Address	Vendor	IP Address	AP Name	Controller	802.11 Rate	SSID	Profile	Authenticated
25.9.2009 10:26	00:15:af:2f:70:20	Asustek	192.168.52	AP0024-o4e-L-F80	MASTONET_200	Associated	KYRVAT	KDE	Yes

KUVIO 19. WCS-palvelimen raporttiesimerkki

7 YHTEENVETO

Keskitetysti hallittavat järjestelmät ovat jo tätä päivää langattomien verkkojen käytön lisääntyessä ja hallittavien järjestelmien kasvaessa suurempiin mittoihin. Valmistajilla on tarjota kontrollereita pienistä WLAN-verkoista suuriin järjestelmiin. Eri valmistajien järjestelmiä vertailtiin onnistuneesti niin teoriassa kuin käytännössäkin. Käytännön testeissä vertailtiin Ciscon ja D-Linkin järjestelmiä joiden välillä lopullinen valinta Mastonet-verkon uusista laitteista tehtiin. Ero laitteistojen välillä oli hiuksen hieno, ominaisuuksissa kontrollereiden välillä ei juuri löytynyt. Tukiasema vaihtoehtoisissa D-Link jäi kilpailijoistaan, mutta kilpailukykyinen hinta kallisti vaakakupia D-Linkin suuntaan. WCS-hallintapalvelimen kaltaisen sovelluksen puute D-Linkin järjestelmästä ratkaisi lopulta valinnan Ciscon laitteiston eduksi.

MESH-verkon laitteita testattiin onnistuneesti. MESH-verkon testien perusteella oli tarkoitus tutkia sen soveltuvuutta toteutettavaksi Mastonet-verkossa. MESH-verkko todettiin varsin toimivaksi järjestelmäksi sekä käyttöä kyllä löytyisi sataman kattamisella WLAN-verkolla. MESH-verkko jäi nyt tässä vaiheessa toteuttamatta laitteiden korkean hintatason vuoksi. MESH-tukiasemien hinnat on nyt tätä kirjoittaessa tullut alaspäin testi- ja vertailuajankohtaan nähden, kun esimerkiksi Ciscon 1240- ja 1130-sarjan tukiasemiin 1520-sarjan lisäksi on tullut saataville tuki MESH verkoille. Testeistä yleisesti ottaen täytyy sanoa näin jälkempäin, on tullut muutama pikku juttu mieleen jota ei tullut testattua tai mitä olisi pitänyt testata toisin, mutta onneksi ei mitään suurta unohtunut.

Ciscon järjestelmän aivan lopullinen käyttöönotto Mastonet-verkkoon jäi vielä tekemättä, koska yhteyttä kaupungin verkkoon, johon kontrolleri tullaan kytkeämään, ei vielä ollut. Järjestelmä saadaan kyllä toimintakuntoon, kunhan vain yhteys kaupungin verkkoon saadaan toimintaan. Kun tarvittavat VLAN-konfiguraatiot saadaan tehtyä verkon muihin laitteisiin, voidaan kontrolleri kytkeä paikalleen ja tukiasemia viedä suunniteltuihin sijoituspaikkoihin. Järjestelmän konfiguraation

todellista onnistumista ei vielä varmasti pysty sanomaan, mutta täytyy olla luottavaisin mielin, että mitään ei ilmene, kun verkkoa aletaan kuormittaa käyttäjillä.

Järjestelmä tuskin tulee pysymään täysin nyt käyttöön otetun kaltaisena oletetun 5-10 vuoden elinaikansa aikana. Voidaan olettaa, että järjestelmän parissa tullaan jatkossakin tekemään opinnäytetöitä, jotka aiheuttavat muutoksia järjestelmään. Järjestelmään tullaan mahdollisesti ottamaan käyttöön uusia palveluita kuten Wishfi-palvelu, jonka mahdollisesta käyttöönotosta on ollut puhetta joka tulisi aiheuttamaan ainakin muutoksia konfiguraatioon. Täytyy toivoa että nyt käyttöönotettava kontrollerijärjestelmä palvelisi ainakin seuraavat viisi vuotta ilman suurempia ongelmia. Tulevaisuudessa nyt käyttöön otettua järjestelmää voidaan laajentaa tukiasema lisenssien loppuessa toisella Ciscon WLAN-kontrollerilla ja kytkeä se WCS-palvelimeen.

LÄHTEET

Calhoun, P., Montemurro, M. & Stanley, D. 2009. RFC5415 Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification 5415 [viitattu 29.11.2009]. Saatavissa: <http://www.rfc-editor.org/rfc/rfc5415.txt>

Cisco Systems, Inc. 2009a. Cisco Wireless Control System Configuration Guide, Release 6.0 [viitattu 29.11.2009]. Saatavissa: <http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/WCS60c.html>

Cisco Systems, Inc. 2009b. Cisco Wireless LAN Controller Configuration Guide, Release 6.0 [viitattu 29.11.2009]. Saatavissa: <http://www.cisco.com/en/US/docs/wireless/controller/6.0/configuration/guide/Controller60CG.html>

Cisco Systems, Inc. 2009c. Cisco Aironet 1130AG IEEE 802.11 A/B/G Access Point [viitattu 29.11.2009]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6087/product_data_sheet0900aecd801b9058.html

Cisco Systems, Inc. 2009d. Cisco Aironet 1240AG Series 802.11A/B/G Access Point Data Sheet [viitattu 29.11.2009]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6521/product_data_sheet0900aecd8031c844.html

Cisco Systems, Inc. 2009e. Cisco Aironet 1250 Series Access Point Data Sheet [viitattu 29.11.2009]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6973/ps8382/product_data_sheet0900aecd806b7c5c.html

Cisco Systems, Inc. 2009f. Cisco Aironet 1520 Series Lightweight Outdoor Access Points [viitattu 29.11.2009]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps8368/data_sheet_c78-532987.html

D-Link Corporation. 2009a. DWS-3000 Series L2+ Unified Wired/Wireless Gigabit Switches [viitattu 29.11.2009]. Saatavissa:

<ftp://ftp.dlink.eu/datasheets/DWS-3024L.pdf>

D-Link Corporation. 2009b. DWL-3500AP Wireless Unified 108G Access Point [viitattu 29.11.2009]. Saatavissa: <ftp://ftp.dlink.eu/datasheets//DWL-3500AP.pdf>

D-Link Corporation. 2009c. DWL-8500AP Wireless Unified 108G Access Point [viitattu 29.11.2009]. Saatavissa: <ftp://ftp.dlink.eu/datasheets//DWL-8500AP.pdf>

IEEE. 2009. Official IEEE 802.11 working group timelines - 11/25/09 [viitattu 27.11.2009]. Saatavissa:

http://www.ieee802.org/11/Reports/802.11_Timelines.htm

Granlund, K. 2007. Tietoliikenne 3. laitos Jyväskylä: Docendo.

Heegard, C. & Shoemake, M. 2004. Packet binary convolutional codes. United States Patent [viitattu 1.12.2009]. Saatavissa:

<http://www.freepatentsonline.com/6823488.html>

Hämäläinen, P. 2005. Runkoverkko langattomasti. Tietokone 5/2005 [viitattu 30.3.2009]. Saatavissa:

<http://www.tietokone.fi/lukusali/artikkelit/2005tk05/kytkentoja.htm>

Leidenius, K. 2008. Wlan kiihdyttää kuitunopeuksiin. Tietokone 13/2008 [viitattu 30.3.2009]. Saatavissa:

<http://www.tietokone.fi/lukusali/artikkelit/2008tk13/tulevaisuudentekniikka.htm>

McKeag, L. 2004. What'sbehind the CAPWAP flap? Techworld 13.4.2004 [viitattu 2.11.2009]. Saatavissa: <http://features.techworld.com/mobile-wireless/480/whats-behind-the-capwap-flap/>

Meru Networks, Inc. 2008a. Meru Controller Installation Guide Release 3.6.

Meru Networks, Inc. 2008b. Meru Access Point and Radio Switch Installation Guide.

Motorola, Inc. 2009a. Enterprise WLAN Infrastructure At-a-Glance [viitattu 29.11.2009]. Saatavissa:

http://www.motorola.com/staticfiles/Business/Products/Wireless%20LAN%20Devices/_Documents/_static%20files/EWLANAAG_BRO_0408.pdf?localeId=33

Motorola, Inc. 2009b. *Motorola SMART Branch* Easy, cost-effective 802.11n wireless networking for branch offices [viitattu 29.11.2009]. Saatavissa:

http://www.motorola.com/staticfiles/Business/Solutions/Industry%20Solutions/wireless-branch/_Documents/_StaticFiles/EWLAN_Branch_Brochure_Web_version_FIN AL.pdf?localeId=33

Mäkinen, I. 2006. Konserninlaajuisen WLAN-verkon suunnittelu. Stadia [viitattu 15.11.2009]. Saatavissa:

https://oa.doria.fi/bitstream/handle/10024/5557/stadia_1159999789_0.pdf?sequence=1

Puska, M. 2005. Langattomat lähiverkot. Helsinki: Talentum.

Viestintävirasto. 2009. Radiotaajuusmääräys 4 [viitattu 27.11.2009]. Saatavissa:

http://www.ficora.fi/attachments/suomiry/511ynJnBp/RTM2009_suomi.pdf

Wikipedia. 2009a. IEEE_802.11 [viitattu 21.3.2009]. Saatavissa:

http://fi.wikipedia.org/wiki/IEEE_802.11

Wikipedia. 2009b. IEEE_802.11 [viitattu 21.3.2009]. Saatavissa:

http://en.wikipedia.org/wiki/IEEE_802.11

Wikipedia. 2009c. IEEE 802.11g-2003 [viitattu 27.11.2009]. Saatavissa:

http://en.wikipedia.org/wiki/IEEE_802.11g-2003

Wikipedia. 2009d. ISM-taajuusalue [viitattu 27.11.2009]. Saatavissa:

<http://en.wikipedia.org/wiki/ISM-taajuusalue>

Wikipedia. 2009e. Wireless mesh [viitattu 21.3.2009]. Saatavissa:

http://fi.wikipedia.org/wiki/Wireless_mesh

Wikipedia. 2009f. Wireless mesh network [viitattu 21.3.2009]. Saatavissa:
http://en.wikipedia.org/wiki/Wireless_mesh_network

Wikipedia. 2009g. WLAN [viitattu 27.11.2009]. Saatavissa:
<http://fi.wikipedia.org/wiki/WLAN>

Wikipedia. 2009h. Capwap [viitattu 27.11.2009]. Saatavissa:
<http://en.wikipedia.org/wiki/CAPWAP>